МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КОБА ВАЛЕРІЙ БОРИСОВИЧ

УДК 343.98: 343.131

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

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

Автореферат
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Дніпро – 2024

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
Степанюк Руслан Леонтійович,
Харківський національний університет внутрішніх справ,
професор кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1;

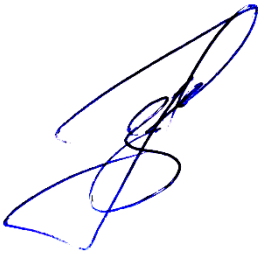
доктор юридичних наук, професор
Чорноус Юлія Миколаївна,
Національна академія внутрішніх справ,
професор кафедри криміналістики та судової медицини.

Захист відбудеться 28 січня 2024 року об 12-00 годині на засіданні спеціалізованої вченої ради Д 08.727.02 Дніпропетровського державного університету внутрішніх справ за адресою: 49005, м. Дніпро, просп. Гагаріна, 26.

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

Автореферат розіслано 26 грудня 2023 року.

Учений секретар
спеціалізованої вченої ради
В.С. Березняк



ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. 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. Шепітько та 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. Добрової, Г. В. Захарової, І. О. Коваленка, О. В. Курмана, В. Р. Мойсика, О. Л. Мусієнко, Н. В. Павлової, В. І. Пазиніч, Д. А. Птушкіна, О. А. Самойленко, Т. Л. Тропіної, 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, окреслив структуру 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 додатків викладено на 42 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** аргументовано актуальність теми дослідження, розкрито рівень вивчення проблематики, зв’язок роботи з науковими програмами, планами та темами, визначено мету і завдання, сформульовано об’єкт і предмет дослідження, охарактеризовано методи і емпіричну основу роботи, з’ясовано наукову новизну та практичне значення отриманих результатів, наведено дані про наявні публікації та апробацію окремих положень дисертації, визначено структуру й обсяг роботи.

Розділ 1 «Наукові засади побудови криміналістичної характеристики шахрайства у сфері е-комерції» складається з чотирьох підрозділів, які присвячено дослідженню стану наукової розробки визначеної проблеми, а також опису ознак окремих елементів криміналістичної характеристики.

У *підрозділі 1.1 «Сфера е-комерції як об’єкт криміналістичного дослідження»* здійснено аналіз ринку електронного бізнесу, як найважливішого сегменту сучасної цифрової економіки, що дедалі частіше привертає увагу ОГ і

стає сферою їх злочинних інтересів. З'ясовано основні напрями і проблемні питання функціонування сфери інтернет-комерції та рівень й характер комерційних угод, що здійснюється у дистанційному форматі.

Окреслено наукові підходи щодо сутності окремих наукових категорій, що характеризують правовідносини у комерційній сфері, зокрема: «електронна комерція», «цифрова торгівля», «електронний бізнес», «електронна торгівля» тощо, які мають різний зміст та наповнення. Доведено необхідність розмежування понять «електронна комерція» і «електронна торгівля», які є складовими електронного бізнесу, оскільки кожне з них має різну змістовну складову.

Визначено коло суб'єктів, які задіяні у цифровому секторі економіки, окреслено характер їхньої взаємодії, функціональне призначення та правовий статус кожного. Здійснено аналіз нормативно-правових актів, що визначають організаційно-правові засади діяльності у сфері електронної комерції в Україні.

Наголошено на збільшенні комерційних угод, які здійснюються у дистанційній формі, особливо у період пандемії COVID-19 та запровадженого воєнного стану. Значне поширення комерційної діяльності у віртуальному просторі стало підґрунтям для збільшення шахрайських проявів. Виникає низка загроз і невирішених проблем, пов'язаних із: 1) колізіями у законодавстві, що регулює електронний бізнес; 2) недостатнім контролем з боку державних органів за діяльністю підприємців, які здійснюють комерційні операції в електронному режимі; 3) порушенням конфіденційності персональних даних; 4) відсутністю дієвої системи захисту електронних баз та інформаційних ресурсів. Виокремлено складнощі, з якими стикаються слідчі у протидії шахрайствам: визначення територіальної підслідності, взаємодія з фінансовими установами, правильна кваліфікація діяння на початку розслідування, відсутність заходів профілактики.

У *підрозділі 1.2 «Способи вчинення шахрайства у сфері е-комерції»* наголошено, що з розвитком суспільних відносин шахрайські дії у сфері е-комерції завжди видозмінюються й модернізуються, шахраї дедалі обирають нетипові способи підготовки, учинення й приховання злочинних дій.

З'ясовано, що *спосіб* шахрайства є головним елементом криміналістичної характеристики та здебільшого має повноструктурний характер (89 %).

Систематизовано підготовчі дії до вчинення шахрайства: 1) обрання напряму комерційної діяльності, де планується здійснювати шахрайські дії; 2) підбір співучасників злочину та обрання схем шахрайських дій; 3) визначення часу, місця й способу шахрайства; 4) підготовка пакету документів для реєстрації суб'єкта комерційної діяльності або підробка документів шляхом внесення до них недостовірних даних; 5) створення фіктивних віртуальних клубів, інтернет-магазинів, фірм із надання різноманітних послуг; 6) створення фіктивних сайтів, аккаунтів; 7) відкриття банківських рахунків для зарахування грошових коштів; 8) створення фіктивної електронної адреси для здійснення переписки з клієнтами комерційних угод; 9) придбання SIM-карток для здійснення переговорів з клієнтами шляхом зміни телефонних номерів; 10) підбір товарів для продажу, створення їх характеристик та наповнення інтернет-магазину інформацією про ці товари; 11) обрання способів здійснення розрахунків та доставки товарів;

12) створення рекламних роликів, портфоліо з демонстрацією успішності комерційних проєктів; 13) розміщення інформації у соціальних мережах про можливості комерційних угод; 14) створення сприятливих умов для шахрайських дій; 15) підготовка засобів злочину (комп'ютерна техніка, фіктивні документи, приміщення з певним цільовим призначенням); 16) налагодження корупційних зв'язків з представниками органів влади й управління, суб'єктами, які мають відношення до супроводження комерційної діяльності в онлайн просторі, та ін.

Визначено типові способи шахрайства. Зосереджено увагу на способах приховування шахрайських дій: знищення технічних пристроїв та інформації, що міститься на електронних носіях (79 %), використання разових номерів мобільних телефонів (81 %), намагання спілкуватися з потерпілим виключно в онлайн-форматі (93 %), фальсифікація доказів (78 %), внесення неправдивої інформації до електронних баз даних (27 %), надання неправдивих показань при проведенні СРД (85 %), застосовування трансформації ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються шахрайські дії (69 %).

У *підрозділі 1.3 «Обстановка та слідова картина шахрайства. Предмет злочинного посягання»* на підставі аналізу наукових праць (Н. М. Ахтирська, Т. В. Романенко, С. В. Чучко) систематизовано та досліджено об'єктивні умови, у яких вчинюються шахрайські дії із застосуванням цифрових технологій.

Розглянуто *обстановку* шахрайства, як сукупності об'єктивних факторів та умов матеріальної обстановки, просторово-часових характеристик місця і часу. Обстановка є найбільш спірним елементом криміналістичної характеристики шахрайства, 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 межі одного регіону або держави, що ускладнює визначення просторово-часових характеристик. Виходячи з цього, 84 % шахрайств у сфері е-комерції не мають чітко окресленого місця події. У вузькому розумінні місцем шахрайства 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 з використанням технології Wi-Fi, місця розташування жертви шахрайських дій. У географічному розумінні 92 % усіх «віртуальних комерційних угод» здійснюється у мегаполісах. При цьому, кількість суб'єктів, які пропонують товари й послуги комерційного призначення, набагато більше, ніж кількість осіб, які потребують таких товарів і послуг, що пояснюється дефіцитом таких об'єктів у невеликих містах. Обстановка обов'язково повинна розглядатися з урахуванням умов, у яких діяв шахрай. З'ясування обстановки шахрайства дозволяє визначити необхідні першочергові СРД і НСРД та подальші напрями розслідування.

Виокремлено *слідову картину* шахрайства. Більшість слідів шахрайських дій відображаються у роздрукованих документах, скриншотах переписки, квитанціях, відтисках печаток і штампів, а також можуть міститися на магнітних носіях і оптичних дисках, флеш-носіях тощо. Інформацію про зовнішність шахрая

може надати потерпілий у випадку безпосередньої зустрічі з ним при укладені комерційної електронної угоди або спілкуванні у форматі відеоконференції.

Приділено увагу віртуальним (електронним, цифровим) слідам, що містяться у мережі Internet (акаунти, web-сторінки, сайти), а також у різноманітних реєстрах та електронних документах. Окреслено *предмет* шахрайського посягання з урахуванням запровадженого воєнного стану.

У *підрозділі 1.4 «Характеристика особи злочинця та потерпілого»* охарактеризовано криміналістично значущі типологічні ознаки особи шахрая та особливості віктимогенної поведінки потерпілих. Шахрайства у сфері е-комерції здебільшого вчиняються у складі ОГ, учасниками якої є: банківські працівники; фахівці з інформаційно-програмного забезпечення; інтернет-провайдери, фінансисти, бухгалтери на комерційних підприємствах; фахові особи, які займаються комп'ютерним шпіонажем; оператори телекомунікаційних послуг.

З'ясовано, що властивою характеристикою шахрая є особливий вид ознак – інтелектуальні. Адже без наявності у особи певних спеціальних вмінь й навичок досить складно реалізовувати відповідні дії (використовувати цифрові технології, здійснювати електронні комерційні операції). Це пов'язано з активізацією процесів використання цифрових технологій та діджиталізації суспільства.

Сформовано типовий «портрет» особи шахрая, що має розшукове значення. З'ясовано, що шахрайства переважно скоюють чоловіки (68 %), більшість з яких мали вищу освіту (62 %), одружені (56 %). Найбільш криміногенні групи становлять особи віком від 25 до 45 років. Зосереджено увагу на структурі ОГ та діяльності її організатора щодо координації дій усіх членів угрупування.

Надано характеристику особі потерпілого. Виокремлено віктимогенні групи осіб щодо яких було вчинено шахрайство і які піддалися впливу шахраїв, а саме: 1) фізичні особи, які виступають потерпілими при здійсненні купівлі-продажу товарів і послуг на онлайн-платформах, інтернет-аукціонах, при здійсненні web-банкінгу; 2) юридичні особи – при здійсненні: господарських операцій між юридичними і фізичними особами; матеріально-технічного постачання з використанням засобів електронної комерції у виробництві; брендингу й просування торгової марки компанії; трансакцій з фінансовими установами між суб'єктами; наданні іншим підприємцям майданчику для створення магазинів і торгівлі своїм товаром (маркетплейси); наданні логістичних послуг та ін.

Розділ 2 «Організаційно-тактичне забезпечення розслідування шахрайства у сфері е-комерції» складається з трьох підрозділів, у яких надано характеристику особливостям початку кримінального провадження, організації розслідування, проведення окремих процесуальних дій, напрямам взаємодії правоохоронних органів, особливостям використання спеціальних знань.

У *підрозділі 2.1 «Криміналістичний аналіз первісної інформації та організація розслідування шахрайства»* визначено підстави початку кримінального провадження, окреслено коло обставин, що підлягають встановленню, та основні елементи організації розслідування. З'ясовано проблемні питання, що виникають під час планування розслідування шахрайства. Наголошено на складнощах визначення кримінально-правової кваліфікації діяння

на початку кримінального провадження, адже одні й ті самі дані про протиправне діяння можуть мати різну кримінально-правову кваліфікацію. Для розмежування «простого» шахрайства (ч. 1 ст. 190 КК) від кваліфікованого (ч. 3 ст. 190 КК) 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 потерпілого. Важливу роль в цьому процесі відіграє ретельний допит потерпілого та витребування в нього з подальшим дослідженням документів (листування в месенджерах або електронній пошті з шахраями, виписки про рух коштів з особистого банківського рахунку, надані операторами зв'язку роздруківки вхідних й вихідних телефонних дзвінків).

Зважаючи на виключно правовий характер цієї проблематики та неоднакове застосування судами норм матеріального права при розгляді справ зазначеної категорії, запропоновано узагальнити судову практику та сформувати єдину правову позицію.

Розглянуто приводи й підстави для відкриття кримінального провадження щодо шахрайства, виокремлено джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт учинення шахрайських дій у кіберпросторі. Окреслено коло обставин, що підлягають встановленню. Охарактеризовано алгоритми отримання інформації від операторів мобільного зв'язку, представників банківських установ та інтернет-провайдерів. Наголошено на важливості встановлення структури ОГ, виявлення її лідера, визначення усіх співучасників шахрайських дій.

Виокремлено типові слідчі ситуації, що виникають на початковому етапі розслідування шахрайства, та визначено відповідні тактичні завдання, які необхідно вирішити у кожній такій ситуації.

Визначено особливості взаємодії слідчих з іншими правоохоронними органами, а також установами, підприємствами та організаціями, громадськістю та ін. Особливу увагу приділено взаємодії слідчого з оперативними службами Департаменту кіберполіції, у тому числі при документуванні діяльності так званих «Call-center». Зосереджено увагу на значенні своєчасного обміну інформацією на початковому етапі розслідування шахрайства як найбільш ефективної форми взаємодії у кримінальному провадженні.

У *підрозділі 2.2 «Організаційно-тактичні особливості проведення окремих процесуальних дій»* з'ясовано, що найбільш поширеними серед СРД та інших процесуальних дій у кримінальних провадженнях є: огляд місця події (98 %); огляд електронної інформації (86 %); тимчасовий доступ до речей і документів (71 %); огляд документів (93 %); обшук (82 %); допит підозрюваного, потерпілого й свідка (100 %); зняття (вилучення) інформації з електронних комунікаційних мереж (49 %); зняття інформації з електронних інформаційних систем (39 %) та ін.

Визначено місця, що найчастіше підлягають огляду. Наголошено на організаційно-тактичній складовій різних видів оглядів, зокрема: місця події, сітьового й серверного обладнання, паперових документів, електронних документів, комп'ютерної техніки, мобільних телефонів, планшетів та ін.

Зосереджено увагу на *огляді електронної інформації*, що розміщена у відкритому доступі у мережі Інтернет, а також такої, що знаходиться на матеріальних носіях інформації і хмарних сервісах зберігання електронної інформації. Визначено 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. З'ясовано, що у разі отримання пароля від власника облікового запису у хмарному сховищі, інформація, що знаходиться у віртуальному форматі, копіюється з сервера на USB-флеш-накопичувач або роздруковується, після чого оглядається. Натомість, якщо авторизаційні дані для доступу до аккаунта у хмарному сервісі отримати не вдалося, здійснюється зняття інформації з електронних інформаційних систем.

Значну увагу приділено НСРД, зокрема: зняттю інформації з електронних комунікаційних мереж, зняттю інформації з електронних інформаційних систем та накладенню арешту на кореспонденцію, її огляду та виїмці.

Зосереджено увагу на тактиці обшуку, адже злочинці заздалегідь вживають заходів щодо знищення або приховання доказової інформації, яка доводить їхню причетність до шахрайських дій. Визначено об'єкти, які підлягають вилученню під час обшуку: 1) реєстраційні документи, що посвідчують законність діяльності суб'єкта комерційної діяльності; 2) фотографії, відеозаписи, на яких міститься інформація, що має значення для справи (факти знайомства певних осіб між собою або перебування особи у певному місці); 3) документи, що відображають особливості комерційної діяльності осіб, які мають відношення до шахрайства; 4) документи, що містять відомості про можливих покупців; 5) електронні й паперові договори про комерційні угоди; 6) документи, що посвідчують особу (підроблені документи на ім'я інших осіб); 7) SIM-картки; 8) квитанції про проведення банківських операцій; 9) мобільні телефони, де містяться адресна книга, смс-повідомлення, фотографії; 10) комп'ютерна техніка (ноутбуки, планшети, системні блоки), де може міститися інформація про шахрайські дії; 11) електронні носії інформації; 12) документи, що підтверджують відкриття розрахункових рахунків у банківській установі; 13) договори з іншими організаціями, підприємствами й приватними підприємцями, які беруть участь у комерційних операціях; 14) печатки й штампи (у т.ч. підроблені), кліше підписів.

Визначено особливості вилучення мобільних пристроїв (телефон, smart-годинник, планшетний комп'ютер, GPS-навігатор, портативний відеореєстратор) у заблокованому і розблокованому станах.

Зосереджено увагу на *тимчасовому доступі до речей і документів*, а також інформації, що перебуває у володінні мобільного оператора, банківських установах, інтернет-провайдерів тощо.

Значну увагу приділено тактиці *допиту* та *одночасного допиту* двох раніше допитаних осіб різної категорії учасників кримінального процесу.

Запропоновано проводити допити потерпілих та оглядати їхні мобільні телефони, планшети, ноутбуки та іншу комп'ютерну техніку, за допомогою якої відбувалося листування або розмова потерпілого з шахраєм. Під час проведення

огляду фіксувати вхідні й вихідні дзвінки, листування, а також іншу необхідну інформацію. При наявності у потерпілого витягу про рух коштів, а також інших документів, долучати їх до матеріалів провадження. Окрім того, під час допиту з'ясовувати номера потенційних злочинців, номера банківських карт, на які здійснювалися перекази коштів, та сайти, на яких розміщувалися оголошення.

Охарактеризовано тактичні прийоми, що найчастіше застосовуються під час допиту підозрюваного: створення уявлення про повну поінформованість слідчого про злочинну подію (61 %), пред'явлення речових і електронних доказів (82 %), демонстрація можливостей щодо подолання системи логічного захисту і входу до комп'ютерних систем (41 %), використання фактора раптовості (71 %) або асоціативних зв'язків (32 %), оголошення показань інших осіб (37 %), використання конфліктів в ОГ (29 %), застосування відеозапису (44 %), участь у допиті спеціаліста (31 %). З'ясовано, особливості допиту членів ОГ, наголошено на проблемних питаннях допиту лідера ОГ та запропоновано шляхи їх вирішення.

У *підрозділі 2.3 «Використання спеціальних знань як засіб тактичного забезпечення розслідування шахрайства у сфері е-комерції»* розглянуто поняття, форми, види і суб'єкти використання спеціальних знань. Визначено процесуальні й непроцесуальні форми використання спеціальних знань. Наголошено на участі спеціаліста при проведенні окремих СРД, зокрема: обшуку, тимчасовому доступу до речей та документів, у ході яких ведеться пошук і вилучається інформація, що міститься на електронних носіях інформації, хмарних сховищах, мобільних телефонах. Визначено алгоритм дій спеціаліста при необхідності подолання системи логічного захисту інформації та входження до комп'ютерних систем, а також огляді комп'ютерної техніки та носіїв електронної інформації.

Не менш важливою є участь спеціаліста при проведенні допиту, особливо, якщо показання надає особа, яка є фахівцем у цифрових технологіях, економічній кібернетиці або компетентною у галузі комерційної чи банківської діяльності, е-бізнесі. Консультативно-довідкова допомога спеціаліста набуває особливого значення, якщо комерційна діяльність відбувалася у дистанційному форматі.

Визначено перелік судових експертиз, що можуть призначатися при розслідуванні шахрайства. З'ясовано особливості підготовки і проведення судових експертиз, зокрема: технічної експертизи документів, почеркознавчої, портретної, телекомунікаційної, трасологічної, комп'ютерно-технічної та експертизи відеозвукозапису тощо.

Розділ 3 «Напрями підвищення ефективності криміналістичного забезпечення розслідування шахрайства у сфері е-комерції» складається з трьох підрозділів, в яких розкрито шляхи оптимізації розслідування через призму тактичних операцій, використання міжнародного досвіду протидії шахрайським проявам та можливих профілактичних заходів уповноважених осіб.

У *підрозділі 3.1 «Тактичні операції як засіб оптимізації розслідування шахрайства у сфері е-комерції»* запропоновано підхід до розгляду методики розслідування шахрайства через призму проведення комплексів тактичних операцій. Визначено теоретичні засади побудови й використання тактичних операцій при розслідуванні шахрайства. Тактичні операції є дієвим засобом

оптимізації діяльності слідчого, що використовується для вирішення комплексу тактичних завдань. Наведено перелік типових тактичних операцій та охарактеризовано особливості застосування. Визначено організаційні заходи до проведення операцій та комплекс дій, що входять до їх змісту.

В межах тактичної операції «Збирання вихідної інформації про шахрайство» запропоновано комплекс заходів, спрямованих на встановлення ознак шахрайства, залежно від певного етапу злочинної діяльності та установлення справжнього наміру особи на момент здійснення електронного правочину. Тактичні операції «Встановлення IP-адреси», «Пошук і викриття шахрая» та «Ідентифікація особи у віртуальному просторі» передбачають проведення комплексу СРД, НСРД та інших заходів, спрямованих на отримання доказів протиправних дій фігурантів, встановлення суб'єктів підприємницької діяльності, які надають телекомунікаційні та послуги хостингу, реєстраторів доменних імен з метою отримання білінгової інформації про клієнтів, способи оплати за хостинг, за доменне ім'я й інших фактів, що дозволяють встановити особу шахрая у віртуальному просторі. Розглянуто проведення тактичної операції «Незаконна транзакція», що полягає у перевірці історії проведених транзакцій, здійснених особами, які є фігурантами у провадженні щодо шахрайства, та виокремленні фактів, що визначають кримінальну відповідальність осіб, які їх здійснювали. Наголошено на необхідності встановлення факту зламу аккаунта та крадіжки персональних даних, які використовувалися для здійснення незаконних транзакцій. Окреслено особливості тимчасового доступу 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, IP-адреси користування web-банкінгом тощо.

Охарактеризовано особливості реалізації СРД, НСРД, організаційно-технічних заходів та інших дій, спрямованих на вирішення тактичних завдань в межах тактичної операції «Фіктивний комерсант». Виявлено комплекс ознак, що можуть свідчити про фіктивність особи, яка здійснює комерційні операції шляхом використання комп'ютерних технологій, зокрема: 1) компанія, що здійснює комерційні операції, або приватна особа-підприємець, не мають відповідного підтвердження про реєстрацію; 2) компанія, що здійснює комерційні операції, або приватна особа-підприємець, зареєстровані на підставну особу; 3) відсутність ідентифікації електронної сторінки з фірмою (наявність ідентифікаційних характеристик компанії, логотипу фірми); 4) компанія, що здійснює комерційні операції, або приватна особа-підприємець, здійснюють продаж інших товарів і послуг, а не тих, щодо яких здійснено домовленість, а також завищують або занижують обсяги угод; 5) комерційні операції не виконувалися особою, яка зазначена їх виконавцем; 6) відсутність на сайті переліку необхідної контактної інформації (контактні телефони, електронна адреса), а також відомостей про діяльність фірми, її товари (послуги); 7) відсутність інформації про успішну реалізацію комерційних проектів.

Наголошено на збільшенні кількості шахрайств, учинених з місць

позбавлення волі, та запропоновано тактичну операцію «Злочинець-в'язень». Реалізація цієї тактичної операції здійснюється у тісній взаємодії слідчого з працівниками оперативних підрозділів Департаменту кіберполіції та співробітниками місць позбавлення волі. Виокремлено тактичні помилки, яких припускаються слідчі при проведенні тактичних операцій.

У *підрозділі 3.2 «Профілактична діяльність уповноважених осіб у провадженнях за фактами шахрайства у сфері е-комерції»* визначено основні напрями й засоби профілактики й запобігання шахрайським діям. Доведено, що профілактична діяльність є одним із основних завдань правоохоронних органів.

Виокремлено причини й умови, що сприяють шахрайству: 1) недосконаліть чинного законодавства та наявність законодавчих колізій щодо здійснення електронних операцій; 2) недоліки у застосуванні кримінального законодавства й неоднозначність судової практики щодо шахрайств, учинених у кіберпросторі; 3) транснаціональний характер шахрайських дій та їх розпливчастість у часі й просторі, що ускладнює їх виявлення; 4) хакерські атаки на сайти, через які здійснюються комерційні операції; 5) сприяння шахрайським діям з боку працівників банку, інтернет-провайдерів, операторів мобільного зв'язку та ін.

Запропоновано спеціальні заходи криміналістичної профілактики. Наголошено на окремій складовій концепції профілактики онлайн-шахрайств – системна діяльність підрозділів кіберполіції щодо моніторингу соціальних мереж та ЗМІ. Зосереджено увагу на використанні можливостей інформаційних ресурсів Національної поліції, в якій створена і тривалий час функціонує система відділів комунікації, які співпрацюють з регіональними та всеукраїнськими ЗМІ, мають власні сайти, web-сторінки в соціальних мережах, виробляють власний аудіовізуальний контент та виявляють високу активність у інших засобах масової комунікації, в т.ч. у соціальних мережах та електронних ЗМІ.

Наголошено на ефективності Всеукраїнської інформаційної кампанії з платіжної безпеки «#ШахрайГудбай», що покликана покращити обізнаність громадян і нагадати про правила безпеки під час безготівкових розрахунків. Така діяльність може здійснюватися через власні канали комунікації Національної поліції, територіальних підрозділів у регіонах (web-портал, Facebook-сторінки, мікроблоги Twitter, Telegram-канали, Instagram-профілі, YouTube-канали, платформи TikTok) або зовнішні (ЗМІ – друковані, Інтернет, ТБ, радіо). З'ясовано суперечності між законодавчим і відомчим рівнями регулювання діяльності слідчих у сфері запобігання шахрайствам, що потребує внесення в чинний КПК положень, які б висвітлювали процедуру здійснення профілактичних заходів.

У *підрозділі 3.3 «Міжнародний досвід протидії шахрайствам у сфері е-комерції»* акцентовано увагу на особливостях запобігання шахрайствам на прикладі зарубіжних країн, зокрема США, Великої Британії та країн ЄС (Німеччина, Нідерланди, Франція, Іспанія). Наголошено на необхідності врахування міжнародного досвіду іноземних держав при створенні національних програм з профілактики шахрайств.

Кібершахрайство є глобальною міжконтинентальною проблемою, а розвиток світової електронної комерції зумовлює збільшення кількості

шахрайських проявів у світовому масштабі. Зосереджено увагу на необхідності своєчасного виявлення й оперативного реагування на кіберінциденти та кібератаки проти електронних інформаційних ресурсів. Наголошено на створенні Єдиної інформаційної системи профілактики шахрайств у сфері е-комерції, яка б поєднувала різноманітні інформаційні ресурси та бази даних про шахраїв.

Акцентовано увагу на важливості постійної міжнародної співпраці у боротьбі з шахрайствами у сфері е-комерції, що ґрунтується на національних законодавчих і підзаконних актах, а також міжнародних угодах, обов'язковість яких підтверджено Верховною Радою України. Здійснено аналіз наявних форм й способів міжнародного співробітництва. Запропоновано напрями надання міжнародної правової допомоги компетентними органами інших держав з питань виконання окремих процесуальних дій, видачі осіб, які вчинили шахрайства, тимчасової передачі таких осіб, перейняття кримінального переслідування тощо.

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 електронні комунікаційні 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 комунікаційних мереж та електронних інформаційних 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 ОПУБЛІКОВАНИХ ПРАЦЬ 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: 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 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.

АНОТАЦІЯ

Коба В. Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-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, 2024.

У дисертації досліджено теоретико-прикладні засади методики розслідування шахрайства у сфері е-комерції. Здійснено аналіз функціонування сфери е-комерції та визначено фактори, які зумовлюють учинення шахрайських дій. Виокремлено елементи криміналістичної характеристики шахрайства. Охарактеризовано типові способи шахрайства. З'ясовано предмет посягання, слідову картину та обстановку шахрайства. Виявлено ознаки шахрая та виділено віктимогенні групи потерпілих. З'ясовано особливості аналізу первісної інформації, кваліфікації шахрайських дій та визначення основних напрямів організації розслідування. Визначено напрями взаємодії слідчих із працівниками кіберполіції, банківських установ, операторами мобільного зв'язку та суб'єктами, які забезпечують передачу і зберігання інформації з використанням інформаційно-комунікаційних систем.

Розкрито тактичні особливості проведення окремих СРД, зокрема: обшуку, огляду, тимчасового доступу до речей та документів, допиту, зняття інформації з електронних комунікаційних мереж та електронних інформаційних систем. Наголошено на сучасних можливостях використання спеціальних знань. Виокремлено тактичні операції: «Збирання вихідної інформації про шахрайство», «Незаконна транзакція», «Встановлення IP-адреси», «Ідентифікація особи у

віртуальному просторі», «Встановлення ознак організованості», «Фіктивний комерсант», «Встановлення умислу», «Затримання» та ін. Для кожної тактичної операції розроблено комплекс дій, спрямованих на вирішення тактичних завдань.

Запропоновано перелік профілактичних заходів, які необхідно здійснювати уповноваженим особам правоохоронних органів для усунення причин і умов учинення шахрайства у сфері е-комерції.

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

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 Internet commerce sphere was carried out and the factors that lead to the commission of fraudulent actions were determined. On the basis of a systematic analysis, the priority areas of combating fraud have been identified.

The main elements of the forensic characteristics of fraud in the field of e-commerce are highlighted. Typical methods of preparing, committing and concealing fraud are identified and characterized, and their classification is proposed. The situation of fraud has been clarified by providing the characteristics of its individual components: the place, time and conditions of fraudulent actions.

The subject of criminal trespass and the trace pattern of fraud have been determined. The focus is on virtual footprints. Forensically significant features of the fraudster were identified, on the basis of which a «portrait» of the alleged criminal was formed. The structure of the organized group is revealed, with the definition of the system of forensically significant features of its members. Victimogenic groups of victims have been identified. The peculiarities of the forensic analysis of primary information, the qualification of fraudulent actions and the determination of the main directions of the organization of the investigation of fraud in the field of e-commerce have been clarified. Tactical operations are singled out: «Collection of initial information about fraud», «Search and exposure of a fraudster», «Establishing an IP-address», «Identification of a person in virtual space», «Establishment of signs of organization», «Episode», «Ensuring compensation for material losses», «Fictitious merchant», «Establishment of intent». For each tactical operation, a set of actions aimed at solving tactical tasks has been developed. A list of preventive measures, which must be carried out by authorized persons of law enforcement agencies in order to eliminate the causes and conditions of committing fraud in the field of e-commerce, is proposed.

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