МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

Рейнгольд Андрій Валентинович

УДК 343.98: 343.131

ДИСЕРТАЦІЯ

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА В ІНТЕРНЕТ-КОМЕРЦІЇ

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

Подається на здобуття наукового ступеня кандидата юридичних наук

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

_____ **А. В. Рейнгольд**

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

Дніпро – 2023

АНОТАЦІЯ

Рейнгольд А. В.Розслідування шахрайства в інтернет-комерції. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. –Дніпропетровський державний університет внутрішніх справ, Дніпро, 2023.

У дисертації на монографічному рівні досліджено теоретичні й практичні положення розслідування шахрайства в інтернет-комерції, з'ясовано сутність їх криміналістичної характеристики у взаємозв'язку її складових елементів.

Наголошено, щокримінальні правопорушення, що вчиняються у кіберпросторі, за різних часів були об'єктом пильної уваги вчених різних галузей знань. Натомість, 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.

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 в

інтернет-комерціїможуть 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.

Розкрито обстановку шахрайства в інтернет-комерції, з урахуванням просторово-часових характеристик, а також умов складної взаємодії комплексу чинників економічного, політичного та соціального характеру.

Зазначено, що місцем учинення шахрайства в інтернет-комерції у широкому розумінні є інтернет-простір, який утворюється завдяки електронним пристроям, підключеним до глобальної мережі інтернет. У вузькому значенні місцем вчинення шахрайства є місцезнаходження електронного технічного засобу (IP-адреса), підключеного до мережі інтернет, а також місце проведення розрахункових операцій (банк, банкомат). Час вчинення шахрайств в інтернет-комерції характеризується досить тривалою подією у часі.

Визначено, що предметом шахрайства в інтернет-комерції 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, маски, апарати штучного дихання, а під час воєнного стану збільшуються випадки, коли предметом шахрайства є речі, необхідні для несення служби у зонах бойових дій (воєнний одяг, бронежилети, каски, 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 тощо).

Сформовано типовий портрет особи шахраяз визначенням соціально-демографічних, біологічних і морально-психологічних ознак.

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.

Визначено характерні підстави для початку кримінального провадження та проблемні питання, які виникають на цьому етапі.Окреслено основні напрями взаємодії слідчого з працівниками Департаменту кіберполіції України та іншими підрозділами Національної поліції, а також представниками служби безпеки Банку (щодо незаконних транзакцій) під час оцінки первинної інформації, що надійшла з відповідних джерел.

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

Наголошено, що в рамках організації розслідування шахрайства, пов'язаного з інтернет-комерцією, 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 кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування та ін.

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.

Вказано типові джерела доказів у кримінальних провадженнях про шахрайства в інтернет-комерції, що враховуються при визначенні слідчих ситуацій та напрямів подальшого розслідування кримінальних правопорушень.

Наголошено, що 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 в інтернет-комерції 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 іншої – 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 або тимчасового доступу до речей та документів у провадженнях щодо шахрайств в інтернет-комерції, зокрема: 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, які 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), які можуть виникати під час проведення процесуальних дій, та надано рекомендації щодо їх усунення.

Висвітлено організаційно-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; які 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 вчинення 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 вчинення шахрайства до звернення громадян до правоохоронних органів чи направлення звернення на електронну скриньку Сервісної служби кіберполіції та ін.

Зосереджено увагу на предметі допиту підозрюваних та осіб, які виступали свідками шахрайських дій. Розглянуто особливості одночасного допиту двох або більше раніше допитаних осіб.

Розкрито організаційно-тактичні особливості пред'явлення для впізнання речей та особи за фотознімками, голосом, в режимі відеоконференції.

Значну увагу приділеноНСРД, 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).

Виокремлено причини й умови, що сприяють учиненню шахрайств в інтернет-комерції, 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 в інтернет-комерції; недоліки в діяльності контролюючих і правоохоронних органів, які своєчасно не виявляють шахрайства в мережі інтернет; наявність законодавчих колізій щодо здійснення комерційних інтернет-угод тощо.

Запропоновано заходи профілактики, що можуть здійснюватися працівниками правоохоронних органів для попередження шахрайств в інтернет-комерції.

Розглянуто міжнародний досвід запобігання комерційним інтернет-шахрайствам, у тому числі й профілактичні заходи, що проводяться Європолом.

Сформовано типові тактичні операції, що проводяться під час розслідування 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.

В рамках вказаних 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, який відіграє важливу роль у реалізації низки тактичних операцій і надає істотну допомогу органам досудового розслідування та підрозділам карного розшуку у виявленні та доведенні фактів шахрайства у мережі інтернет.

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

Ключові слова: *інтернет-комерція, торгівля, мережа інтернет, кримінальні правопорушення, шахрайство, дистанційна угода, криміналістична характеристика, товари, послуги, досудове розслідування, слідча ситуація, слідча версія, слідчі (розшукові) дії, криміналістична профілактика.*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані 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.

SUMMARY

Reinhold A. V. Basics of fraud investigation methods in Internet commerce. – *Qualifying scientific work on the rights of 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 examines the theoretical and practical provisions of the investigation of fraud in Internet commerce, the essence of their forensic characteristics in the relationship of its constituent elements is clarified.

It is emphasized that criminal offenses committed in cyberspace have been the object of close attention of scientists in various fields of knowledge at different times. On the other hand, in none of the scientific works, the issue of the peculiarities of the legal regime of conducting commercial transactions on the Internet and its influence on the formation of the forensic characteristics of commercial Internet fraud has not been considered in detail. The organization and tactics of documenting criminal activities related to commerce in the Internet space also need to be refined and highlighted in a new dimension.

Issues regarding the specifics of the organization and tactics of conducting NSRD, as well as the implementation of tactical operations in fraud proceedings related to Internet commerce, are also insufficiently clarified. Measures of forensic

fraud prevention also remain unexplored, which requires a thorough study, improvement and further development of the specified aspects.

A forensic analysis of fraud in Internet commerce was carried out and the location of each element of the forensic characteristics of such a criminal offense was determined. It is emphasized that theoretical provisions and practical recommendations for the investigation of fraud in Internet commerce can be more well-argued in the case of taking into account the peculiarities of the legal regime regulating relations between various subjects involved in the conclusion of distance agreements; characteristics of these entities; the subject of a criminal offense; circumstances and conditions in which fraud is committed; method of fraudulent actions. Trace information about a criminal event is of special forensic importance.

The situation of fraud in Internet commerce is revealed, taking into account the spatio-temporal characteristics, as well as the conditions of the complex interaction of a complex of factors of an economic, political and social nature.

It is noted that the place of fraud in Internet commerce in the broadest sense is the Internet space, which is formed thanks to electronic devices connected to the global Internet network. In the narrow sense, the location of the fraud is the location of the electronic technical device (IP address) connected to the Internet, as well as the place of payment operations (bank, ATM). The time of committing fraud in Internet commerce is characterized by a rather long event in time.

It was determined that the subject of fraud in Internet commerce is both property - things, money, securities (92 %), and services – insurance, employment, transportation, purchase of tickets for railway or air transport (8 %). On the other hand, as a result of the Covid-2019 pandemic, drugs for this disease, masks, artificial respiration devices began to appear as the subject of encroachment in the proceedings regarding fraud in online commerce, and during the martial law there are increasing cases when the subject of fraud is things necessary for carrying out the service in combat zones (military clothing, body armor, helmets, military equipment, generators, etc.).

The main actions that fraudsters resort to when preparing and committing fraud in Internet commerce are defined, namely: development of the site design, layout of its web pages and its programming; posting of information in social networks; filling the pages of the online store with photos and other characteristics of goods and services; maintenance of advertising of goods and services in order to interest the population; involvement of potential victims in the distance commerce process; use of payment instruments to transfer funds or pay for goods and services; taking possession of goods, services or money without fulfilling the terms of the contract concluded in remote format.

Ways of concealing fraud in Internet commerce, including in the conditions of martial law, are highlighted.

A specific mechanism of trace formation was revealed. Special attention is paid to informational (virtual) traces that can be detected during the study of computer equipment, as well as contained in the Internet (web pages, sites, e-mails, personal profiles, etc.).

A typical portrait of a fraudster has been created with the definition of socio-demographic, biological and moral-psychological features.

Special attention is paid to the characteristics of the victim and the level of victim behavior. Victimhood is manifested in the trustworthiness of entities that offer goods and services in a remote format.

Characteristic grounds for starting criminal proceedings and problematic issues that arise at this stage are determined. The main areas of interaction of the investigator with employees of the Cyber Police Department of Ukraine and other units of the National Police, as well as with representatives of the Bank's security service (regarding illegal transactions) during the assessment of primary information received from relevant sources are outlined.

It is noted that the effectiveness and quality of solving tactical tasks depends on the correct organization and planning of the investigation process, which includes a set of necessary measures that ensure the activity of pre-trial

investigation bodies for the detection, investigation and prevention of criminal offenses at various stages of the investigation.

Attention is focused on the need to define tactical tasks and choose ways to implement them within the framework of organizing and planning the investigation of fraud in Internet commerce. A list of general and private versions and the range of circumstances to be established in this category of criminal proceedings is proposed.

It was emphasized that an important role is played by international cooperation with the competent authorities of other states in the framework of the organization of the investigation of fraud related to Internet commerce in the form of requests, appeals regarding the need to carry out certain procedural actions, delivery of documents, extradition of persons who have committed a criminal offense, temporary transfer of persons, taking over criminal prosecution, etc.

The analysis of scientific developments of scientists regarding the concept, essence and types of investigative situations was carried out. Typical investigative situations of fraud investigation in Internet commerce are formulated and algorithms of actions of law enforcement agencies are determined in accordance with each of them.

Typical sources of evidence in criminal proceedings about fraud in Internet commerce are indicated, which are taken into account when determining investigative situations and directions of further investigation of criminal offenses.

It is emphasized that the specificity of procedural actions aimed at obtaining information from material sources (inspection, search, temporary access to things and documents) is due to the fact that during the investigation of fraud in Internet commerce, there is a need to identify, fix and remove a number of material objects. entities that have evidentiary value. In addition, the mechanism of fraudulent actions is associated with the use of a number of electronic media that reflect information about the transaction, and the implementation of a number of operations that take place through electronic and telecommunication networks.

On the one hand, the received information can contribute to the establishment of certain facts regarding the execution of the transaction, on the other hand, paper and electronic documents, as well as computer equipment can act as material evidence in criminal proceedings.

The list of objects to be seized during a search or temporary access to things and documents in proceedings related to fraud in Internet commerce is given, in particular: computer equipment and software (67 %), technical means of telecommunications (91 %), settlement documents (43 %) and others.

The organizational and tactical features of the extraction and inspection of such computer information carriers are determined. Tactical methods are considered, including those aimed at preventing damage and destruction of information located on physical computer media and in «cloud» storage.

It is proven that the investigator often encounters technical and programming difficulties that require the intervention of knowledgeable persons (programmer, system engineer). The forms of participation of these persons during the search, inspection and temporary access to things and documents are outlined. An algorithm of actions during the examination of a local computer tool is proposed. Non-typical situations (complications) that may arise during procedural actions are summarized, and recommendations for their elimination are provided.

The organizational and preparatory measures for the interrogation of the suspect, the victim and the witness are highlighted. A list of circumstances to be established during the questioning of the victim has been created, in particular: by which means of remote communication the victim learned about the product or service (telecommunications networks, television, Internet); whether attention was paid to studying the reputation of the seller; whether an electronic signature was imposed to secure the agreement; what exactly was advertised, the main characteristics of the products, were there any photos of the product; what were the conditions of sale (payment, delivery); how the communication took place for the purpose of discussing the subject of the contract (telephone or video communication, SMS communication); whether the victim remembered the

appearance of the person who turned out to be a fraud (during the video call); whether the victim made screenshots of the monitor screen (online store), communication with the fraudster; how the user was authenticated and authorized; what was the confirmation of the execution of an electronic transaction (whether the conditions and procedure for exchanging or returning goods or refusing to perform work or providing a service were indicated; whether the details of the seller were indicated; whether warranty obligations and information about other services related to the maintenance or repair of the product or the performance of work or the provision of the service are indicated; whether there is information about termination of the contract; how the victim was paid for the product or service; whether the bank details provided to the victim correspond to those posted on the official website; how the victim realized that the terms of the commercial contract for the sale of goods (services) in the online mode were not fulfilled; whether the victim made claims and how the fraudsters reacted to these claims; whether there was a request to send the goods by cash on delivery; how much time passed from the moment the fraud was committed to the appeal of citizens to law enforcement agencies or the sending of an appeal to the e-mail box of the Cyber Police Service Service, etc.

Attention is focused on the questioning of suspects and persons who witnessed fraudulent actions. The features of the simultaneous interrogation of two or more previously interrogated persons are considered.

The organizational and tactical features of the presentation for the recognition of things and persons by photographs, voice, in the video conference mode are revealed.

Considerable attention was paid to NSRD, which have the greatest specificity in criminal proceedings regarding fraud in Internet commerce, in particular: removal of information from electronic communication networks (76 %), removal of information from electronic information systems (75 %), establishing the location of radio equipment, radio electronic means (91 %) and others. The prevalence of such NSRDs is due to the fact that communication

between the fraudster and the victim, especially during the preparation for committing fraudulent acts, mostly takes place through transport telecommunication networks and the Internet (text messages, video communication, correspondence through an email address, etc.).

The reasons and conditions contributing to fraud in Internet commerce are singled out, in particular: excessive credulity and safety of citizens; negligent attitude to the study of information contained in electronic form regarding the conditions of purchase and sale of goods and services; lowering the standard of living of the population and giving preference to citizens to conclude distance agreements regarding the purchase and sale of goods and services; the prevalence of unreliable offers in the mass media and the Internet; imperfect legal framework for limiting advertising that contains suspicious content, as well as determining the grounds for blocking relevant Internet resources; professional and moral deformation of business entities involved in online trade; the difficulty of proving the fact of fraud on the Internet and the ambiguity of the court's legal positions regarding fraud in Internet commerce; shortcomings in the activities of controlling and law enforcement agencies, which do not detect fraud on the Internet in a timely manner; the presence of legislative conflicts regarding the implementation of commercial Internet agreements, etc.

Preventive measures that can be implemented by law enforcement officers to prevent fraud in Internet commerce are proposed. The international experience of preventing commercial Internet fraud is considered, including preventive measures carried out by Europol. Formed typical tactical operations conducted during the investigation of fraud in Internet commerce, in particular: «Fake site», «Illegal transaction», «Establishment of IP address», «Identification of a person in virtual space», «Establishment of intent», «Organization arrest of a fraudster who operated on the Internet» and others.

Within the framework of the specified tactical operations, the system for detecting fraudulent operations by checking against various filters was considered; the specifics of the analysis of the database of completed transactions; the

possibility of establishing the location of the Internet access point and the provider that facilitated access to the Internet, features of access to information contained in the mailbox, etc. A complex of actions included in the content of tactical operations in criminal proceedings for the investigation of fraud in Internet commerce is defined.

The role of the Cyber Police Department, which plays an important role in the implementation of a number of tactical operations and provides significant assistance to pre-trial investigation bodies and criminal investigation units in detecting and proving facts of fraud on the Internet, is emphasized.

A list of tactical errors and miscalculations made by investigators during the specified tactical operations is defined.

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

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані 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.

ЗМІСТ

Перелік умовних скорочень……..…….....23
ВСТУП ……...24
РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА ВІНТЕРНЕТ-КОМЕРЦІЇ…….……
…….34
1.1. Стан наукових досліджень проблем боротьби із кібер-шахрайством та правові передумови виникнення інтернет-комерції……..34
1.2. Концептуальні основи щодо формування криміналістичної характеристики шахрайства в інтернет-комерції…….……..49
Висновки до 1 розділу……...…71

РОЗДІЛ 2
ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ШАХРАЙСТВА В ІНТЕРНЕТ-КОМЕРЦІЇ…….……
…….74

2.1. Оцінка первинної інформації на початку кримінального провадження...74
2.2. Організація та планування розслідування шахрайства в інтернет-комерції, та коло обставин, що підлягають встановленню……...85
2.3. Типові слідчі ситуації, що виникають під час досудового розслідування шахрайства в інтернет-комерції…….105
Висновки до розділу 2…….118

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО-ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ ШАХРАЙСТВА ВІНТЕРНЕТ-КОМЕРЦІЇ…….122

3.1. Організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій ……..……...122
3.2. Криміналістична профілактика у кримінальних провадженнях за фактами вчинення шахрайства в інтернет-комерції……....148
3.3. Застосування тактичних операцій під час розслідування шахрайствавінтернет- комерції……..…170

Висновки до 3 розділу……....184

ВИСНОВКИ …….……..…….....187

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …….…….....196

ДОДАТКИ ….…….....222

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ГУНП	–	Головне Управління Національної поліції
ГК		Господарський Кодекс
ЄРДР	–	Єдиний реєстр досудових розслідувань
ЗМІ		Засоби масової інформації
КК	–	Кримінальний кодекс
КПК	–	Кримінальний процесуальний кодекс
МВС	–	Міністерство внутрішніх справ
ОГ		Організована група
ОРЗ		Оперативно-розшукові заходи
СОГ	–	Слідчо-оперативна група
СУ		Слідче управління
СРД	–	Слідчі (розшукові) дії
НСРД	–	Негласні слідчі (розшукові) дії
ЦК		Цивільний Кодекс

ВСТУП

Обґрунтування теми дослідження.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. Шепітьката 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 методзастосовано при виокремленні віктимогенних груп потерпілих, класифікації способів шахрайства та типових слідчих ситуацій (підрозділ 1.2, 2.3). Соціологічні методи застосовано прианкетуванні 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 **с**прияли 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 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 видуань (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 сторінках, 4 додатки викладено на 29 сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА В ІНТЕРНЕТ-КОМЕРЦІЇ

1.1. Стан наукових досліджень проблем боротьби із кібер-шахрайством та правові передумови виникнення інтернет-комерції

Основною тенденцією розвитку сучасного суспільства стало широке залучення інформаційної мережі Інтернет до сфери підприємницької (комерційної) діяльності. Це сприяло активному розвитку електронної комерції. Стрімкий розвиток електронної комерції зумовлений значною кількістю переваг, що отримують споживачі, при замовлені товарів та послуг через Інтернет. До них відносять: низьку собівартість придбання товарів з розширенням кордонів бізнесу і виходом на міжнародний ринок. Такий ринок не має часових обмежень, що істотно збільшує реалізацію товарів (послуг) і доходи, створення робочих місць для кваліфікованої робочої сили. Споживачеві електронна комерція дає переваги купувати дешеві товари з економією часу на пошук. Значно знижуються витрати, пов'язані з обміном інформацією за рахунок використання більш дешевих засобів телекомунікації. Внаслідок світової кризи, яка була спричинена пандемією Covid – 19, місцем для отримання прибутку стали чисельні соціальні мережі, інтернет-магазини, маркетплейси (онлайн-ринок електронної комерції). Так, більшість компаній світу, як великих і малих, здійснюють підприємницьку діяльність саме через мережу Інтернет, що дозволяє їм продавати товар та пропонувати свої послуги споживачам у більших масштабах і більшому асортименті, покращуючи при цьому якість обслуговування клієнтів і зменшуючи свої витрати [182, с. 178].

Шахрайства з використанням інтернет-технологій набувають все більш широкого масштабу і охоплюють не тільки інтернет-простір нашої держави, а

й мають навіть міжнародний характер [180]. При цьому, розвиток інтернет-технологій, глобальної і локальних мереж дозволили підняти на новий інтернаціонально-континентальний рівень торговельно-економічні відносини та електронну комерцію. Еволюціонували, зміцнившись, і позиції транснаціональної злочинності, набули нових рис, необмежених можливостей [209, с. 63].До того ж, спостерігається активна інтеграція банківської системи України в світове банківське співтовариство [224, с. 221].Як наслідок цього, міжнародне співтовариство занепокоєне поширенням та ростом шахрайств у електронній торгівельно-комерційній сфері, адже збитки від даного виду кримінальних правопорушень завдають шкоди не тільки продавцям та споживачам, а й економікам цілих країн [80, с. 221].

Шахрайство у сфері електронної торгівлі – один із видів корисливої злочинності, системоутворюючою ознакою якого виступає спільна корислива мотивація до незаконного збагачення та спрямованість злочинної поведінки на заволодіння матеріальними благами у різний спосіб або отримання іншої незаконної вигоди, характеризується значною поширеністю, багатомільйонними збитками, організованим характером, а також складністю його виявлення та запобігання [37, с. 17].

При цьому розвиток електронної торгівлі відбувається у двох напрямах: 1) зростає кількість інтернет-користувачів, які зацікавлені покупкою товарів зазначеним способом (збільшення попиту); 2) збільшується кількість інтернет-магазинів, а лідери ринку розширюють діяльність, впроваджують нові технології, удосконалюють асортимент (збільшення пропозиції) [68, с. 117].

Використання в комерційній діяльності та повсякденному житті найновіших комунікацій та технологій сприяло виникненню таких нових економічних понять, як «електронна комерція», «електронна торгівля». При цьому, згідно Закону України «Про електронну комерцію», електронна комерція – відносини, спрямовані на отримання прибутку, що виникають під

час здійснення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно - телекомунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру [61],а електронною торгівлею вважається господарська діяльність у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом покупцю шляхом здійснення електронних правочинів із використанням інформаційно-телекомунікаційних систем [110; 61].

Не дивлячись на те, що електронна комерція тісно асоціюється саме з електронною торгівлею і, в першу чергу, з онлайн-магазинами, остання, будучи складовою електронної комерції, включає лише відносини купівлі-продажу товарів [51]. Тобто, поняття «е-комерція» ширше, ніж поняття «електрона торгівля», оскільки воно охоплює усі види електронної і комерційної діяльності. Це обмін матеріальних або віртуальних товарів і послуг на гроші (електронні) між об'єктами комерційної діяльності в мережі Інтернет, при чому весь цикл комерційної трансакції або її частина здійснюється електронним способом. Електронна комерція може відбуватися між суб'єктами підприємництва під час виробництва і продажу товарів (бізнес-бізнес), між суб'єктом підприємництва і споживачем, під час продажу і розповсюдження товарів (бізнес-споживач), між двома споживачами (споживач-споживач) [177, с. 33]. Натомість, як зауважують О. Л. Андронік та А. В. Воронін, використання терміну «електронна торгівля» відповідає поняттю «електронна комерція» у вузькому сенсі, враховуючи тільки покупку чи продаж товарів або послуг у мережі Інтернет, замінюючи і доповнюючи традиційні способи взаємодії покупців і продавців, переносячи їх в електронний простір [2, с. 120]. З цього приводу В. Рєзнікова пояснює, що терміни «електронна торгівля» і «електронна комерція» в економіко-правовій доктрині застосовуються рівнозначно, адже ці терміни фактично виникли у зв'язку з тим, що перекладачі документів ООН в сфері електронної комерції з англійської мови використали термін «торгівля», хоча в усьому світі

використовується термін «комерція» [150, с. 60].При цьому, електронна комерція передбачає: відкриття Web-сайтів компанії і віртуальної крамниці в Internet; наявність автоматизованої системи управління процесами; використання електронної реклами і маркетингу; використання певної моделі бізнес-взаємодії [188, с. 8].

З цього виходить, що електронну комерцію можна розглядати у вузькому і широкому значені. У вузькому значенні при здійсненні електронної комерції акцент робиться на операціях з купівлі та продажу товарів та послуг онлайн. У широкому значенні електронна комерція – це підприємницька діяльність яка включає всю ділову активність, що відбувається через мережу Інтернет, а саме: продаж або покупка товарів та надання послуг, онлайн діяльність із маркетингу, переказ коштів, а також збір та обробка даних і надання певних видів інформації щодо проведення такої діяльності [182, с. 179].

Електронна комерція є складовою частиною цифрової економіки, способом її практичної реалізації, що на сьогодні найбільш динамічно розвивається. За своєю природою електронна торгівля є продуктом сучасного розвитку Інтернет-технологій. Під електронною комерцією пропонується розуміти будь-який вид торговельно-підприємницької, торговельної, комерційно-посередницької діяльності, участі у торгівлі, продажу товарів, нерухомості, цінних паперів, наданні послуг з метою одержання прибутків, який здійснюється дистанційним способом із використанням інформаційно-телекомунікаційних систем [179, с. 9].

Натомість, поряд із поняттям «електронна комерція» існують й інші поняття [86, с. 19].До того ж, більшість науковців ототожнюють електронну комерцію з такими поняттями, як «електронний маркетинг», «інтернет-маркетинг», «інтернет-комерція», «електронний трейдинг» [215].

Хоча термін «інтернет-комерція» і не є офіційно визнаний законодавством, що регулює торгівельні відносини в Інтернет просторі, вважаємо, що цей термін є цілком синонімічним терміну «електронна

комерція». Тому у дослідженні пропонуємо використовувати як термін «електронна комерція», так і термін «інтернет-комерція».

Адже інтернет-комерція фактично і є комерційною діяльністю в Інтернеті, коли процес купівлі/ продажу товарів або послуг (весь цикл комерційної/ фінансової транзакції або її частина) здійснюється в електронній формі із застосуванням Інтернет-технологій. При цьому, процесами, які становлять цикл електронної (інтернет) комерції, є: доступ до інформації, оформлення замовлення, оплата, виконання замовлення, після продаж не обслуговування і підтримка [10; 118, с. 343].

Таким чином, можна сформулювати авторське визначення інтернет-комерції – це процес купівлі-продажу товарів та послуг, який здійснюється між реалізаторами і замовниками таких товарів та послуг, за опосередкованою участю третіх осіб (операторів і провайдерів телекомунікаційних послуг, банків та ін.) за допомогою інформаційно-комунікаційних технологій, результатом якого є правочин, укладений в електронній формі.

Цю думку підтримує й Ю. В. Білоусов та О. Ю. Черняк, які вважають, що для даних правовідносин доцільним є використання саме терміна «електронна комерція», а не «електронна торгівля», оскільки, обмежуючи таку діяльність виключно торгівлею, ми спонукатимемо до обмеження ринку робіт та послуг у цій сфері, що не відповідатиме вимогам норм європейського законодавства в цій сфері, зокрема, Директиві 2000/31/ЄС Європейського парламенту та Ради від 8 червня 2000 року про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку («Директива про електронну комерцію») [18, с. 190].

Загалом, трактуванням Комісії ООН з права міжнародної торгівлі ЮНСІТРАЛ нині до електронної комерції відносять такі форми господарської діяльності: електронний обмін інформацією (Electronic Data Interchange, EDI); електронний рух капіталу (Electronic Funds Transfer, EFT); електронну торгівлю (e-trade); електронні гроші (e-cash); електронний маркетинг

(e-marketing); електронний банкінг (e-banking); електронні страхові послуги (e-insurance) [232, с. 117].

При цьому, слід акцентувати увагу, що здебільшого кожний із наведених термінів розглядається сьогодні з різних позицій, зокрема, і економічних, і соціальних, і правових [141].

До того ж, основним засобом регулювання тих чи інших суспільних відносин у кіберпросторі постає відповідне право: інформаційні відносини підлягають регулюванню інформаційним правом; відносини з приводу інтелектуальної власності – інтелектуальним правом; майнові та особисті немайнові відносини – цивільним, господарським правом; відносини, що виникають унаслідок учинення злочину та відкриття відповідного кримінального провадження – кримінальним та кримінальним процесуальним правом [154, с. 16].

У зв’язку із чим проблема боротьби із комерційним інтернет-шахрайством має комплексний і міждисциплінарний характер. Тому вважаємо необхідним охопити низку галузей знань, в межах яких проводилися дослідження з даної проблематики.

У світлі сучасних наукових розробок, що покликані забезпечити ефективне функціонування державної системи щодо запобігання шахрайству, мають враховуватись як сучасні базові правові норми національного законодавства України, які фактично стали результатом запровадження міжнародних правових стандартів у даній сфері, так і цінний доробок вітчизняних науковців, які протягом попередніх років працювали над зазначеною проблематикою. Вивчення сучасного стану наукових робіт, присвячених окремим проблемам запобігання шахрайству, підтверджує тезу про те, що напрями наукових досліджень є актуальними для предмета дослідженнях. Тому різні аспекти запобігання шахрайству підрозділами Національної поліції МВС України є предметом дослідження фахівців у сфері кримінального права, кримінології, кримінально-виконавчого права як вітчизняних, так і зарубіжних науковців [62, с. 26].

Слід сказати, що у низці робот приділяється увага цивільно-правовим відносинам у галузі електронної комерціалізації, правовому режиму регулювання правових відносин у мережі Інтернет.

Так, стану та перспективам розвитку споживчого законодавства України присвячені наукові дослідження О. Ю. Черняк та Ю. В. Білоусова [202; 18].У свою чергу, детермінанти розвитку електронної комерції в умовах глобальної дигіталізації дослідив у своїй дисертації Я. С. Тертичний. Вчений систематизував напрями інтеграції цифрових технологій у ланцюги створення вартості у глобальному бізнесі; визначив сутність та особливості функціонування електронної комерції; дослідив світові тенденції інтеграції інформаційно-комунікаційних технологій в організацію діяльності міжнародних компаній; проаналізував глобальні тренди розвитку електронної комерції в контексті інформаційної глобалізації; визначив канали впливу електронної комерції на інклюзивність економічного розвитку; розробив підходи до моделювання бізнес-процесів віртуальної організації тощо [179, с. 9].

Питанням правового регулювання електронної торгівлі присвячені дисертації М. М. Дутова, А. В. Чучковської та В. М. Желіховського [50; 207; 57].Водночас, у дисертаційному дослідженні І. Б. Бєлік розглянуті питання правового регулювання оподаткування електронної комерції», а вже О. Ю. Кирилюк приділила увагу договорам, що укладаються з використанням електронних засобів зв’язку» [14; 71].

О. І. Шалева розкрила суть, зміст та роль електронної комерції в сучасному секторі світової та вітчизняної економіки, розглянула інструментарій електронної комерції на базі глобальної мережі Internet, сфери та основні принципи ведення електронної комерції. Значну увагу приділила характеристиці основних форм та проектів електронної комерції (зокрема електронним магазинам, електронним аукціонам, електронним торговельним майданчикам) електронним платежам, специфіці надання окремих видів

послуг; висвітлила питання аналізу ефективності електронної комерції та її нормативно-правового забезпечення [208].

Заслуговують на увагу надбання Н. Є. Блажівської, яка сформулювала поняття електронного правочину, довела, що оскільки вчинення електронних правочинах переважно пов'язане із здійсненням певної підприємницької діяльності власника програми-робота, то й ризик несанкціонованого втручання повинен покладатись на нього, за винятком умислу особи-користувача або ж інших випадків, що передбачені законом чи договором. Вчена дійшла висновків, що електронний документ (наприклад, повідомлення з електронної пошти, телефону, у соціальній мережі тощо) може бути прийнятним як доказ у ході судового розгляду справи за умови, що сам документ та особа, яка його направила, а також її вільна воля на вчинення відповідного правочину не викликають сумніву; вона обґрунтувала, що саме поняття «електронний підпис», на відміну від інших суміжних понять, забезпечує найповнішу ідентифікацію сторони електронного правочину та засвідчує цілісність та незмінність самого електронного правочину. У її роботі вказується на необхідність закріплення права споживача на укладання будь-якого дистанційного контракту та на забезпечення інформацією про істотні умови дистанційного контракту [19].

Деякі роботи присвячені адміністративно-правовому регулюванню державного управління у сфері господарської діяльності в Україні. У цьому контексті імпонує думка С. І. Бевз, який поряд із загальними питаннями регулювання державного управління у сфері господарської діяльності, розглянув ще й особливості, пов'язані із впровадженням електронного укладання правочинів стосовно сфери господарської діяльності [11].

Аналіз наукових праць у цьому напряму свідчить, що вченими цивільно-правового та адміністративного напряму в основному приділялася увага розвитку правового регулювання відносин у сфері електронної комерції та вдосконаленню таких правовідносин. Безумовно, низка положень може бути покладена в основу побудови методики розслідування шахрайств у сфері

інтернет-комерції при визначенні факторів, які зумовлюють зловживання у цій сфері, при розумінні механізму здійснення комерційних операцій у дистанційному варіанті тощо. Питання ж вчинення шахрайських дій при здійсненні електронної комерції у вказаних роботах розглядалися лише фрагментарно.

Разом з цим, ускладнення криміногенної ситуації зумовило необхідність цільових досліджень у напрямі розроблення та впровадження в практичну діяльність правоохоронних органів системи заходів щодо запобігання шахрайствам і іншим злочинам проти власності. Ураховуючи сучасний стан криміногенної обстановки в державі, складну економічну й суспільно-політичну ситуацію, запобігання злочинам проти власності є предметом дослідження багатьох вітчизняних учених-кримінологів [20, с. 23].

Протидія та запобігання кіберзлочинності в Україні, її правові та організаційні засади розглядаються у роботах О. Є. Користіна, В. М. Бутузова та В. В. Василевича [146].

Особливої уваги заслуговує дисертація О. І. Кривенко, який визначив організаційно-тактичні особливості протидії шахрайствам через мережу Інтернет та охарактеризував оперативно-розшукову характеристика вказаних злочинів, перспективні шляхи вдосконалення законодавства з окресленого питання [87, с. 3].

С. І. Афанасенко окремою проблемою визнав віктимізацію відносин громадян, що призводить до збільшення кількості шахрайств. У своїй дисертації «Віктимологічна профілактика шахрайства» (2013 р.) вчений визначив ключові проблеми віктимологічної профілактики шахрайських посягань, зокрема: жертви шахрайства, віктимологічна детермінація шахрайства та особливості механізму віктимної поведінки осіб, щодо яких вчиняється шахрайство; дослідив основні напрями загальної, спеціально та індивідуальної віктимологічної профілактики, як системи заходів з боку державних органів, громадських організацій, окремих осіб, що спрямовані на

усунення причин та умов віктимізації та перетворення особи на жертву злочину тощо [7, с. 13].

Особливості предмета доказування у кримінальних провадженнях про економічні злочини та їх вплив на методику розслідування розглянуті у роботі О.В. Пчеліної [149].А вже питання кримінальної відповідальності за дії, пов’язані із обманом та зловживанням довірою висвітлюються у роботі О.В. Смаглюк та Ю. Л. Шуляк, які провели юридичний аналіз основних і кваліфікованих складів шахрайства, визначив критерії відмежування складу шахрайства від суміжних злочинів [162; 216].

Слід зауважити, що в рамках формування методики розслідування шахрайств, пов’язаних із електронною комерцією, особливу цінність становлять праці, в яких висвітлюються питання щодо методики розслідування шахрайств, а також суміжних із ними злочинів, у тому числі злочинів економічної спрямованості [95].Наукові основи комплексної методики розслідування економічних злочинів заклав у своїй докторській дисертації А. Ф. Волобуев [31].

Одним із перших висвітлив актуальні проблеми розслідування шахрайства в сучасних умовах О. Л. Мусієнко. Ним проаналізовано психологічний механізм реалізації злочинного діяння при вчиненні шахрайства; розкрито зміст криміналістичної характеристики шахрайства, визначено види та способи даної категорії злочинів; типізовано слідчі ситуації і основні напрямки розслідування, запропоновано слідчі версії; розглянуто особливості тактики проведення слідчих дій при розслідуванні шахрайства [113].

Заслуговує на увагу наукова діяльність С. С. Чернявського, який охопив достатньо широкий спектр проблем, пов’язаних із розслідуванням шахрайства. Об’єктом уваги вченого стала й сфера банківського кредитування [201], без участі якої не відбувається жодний електронний правочин.

Не залишилася без уваги й сфера господарсько-договірних зобов'язань. Так, Є. В. Дехтярьов у своїй дисертації визначив загальні засади методики розслідування шахрайств у сфері виконання господарсько-договірних зобов'язань і сформулював рекомендації, спрямовані на вдосконалення й оптимізацію діяльності слідчих і оперативних підрозділів щодо виявлення та розслідування даної категорії злочинів; визначив особливості розв'язання типових слідчих ситуацій початкового етапу розслідування, відшкодування збитків, завданих вчиненням злочину та проаналізував специфіку проведення окремих слідчих (розшукових) дій [41].

Побудові побутових відносин між потерпілим та злочинцем в результаті здійснення шахрайських цивільно-правових правочинів присвячена робота Н. Ю. Кириленко [70; 95].

Фрагментарно охоплюються шахрайства, що вчинені в мережі Інтернет, у дисертації К. Д. Заяць, який розробив криміналістичну класифікацію шахрайств; виокремив всі прояви шахрайства на наступні групи: 1) шахрайства, що вчиняються під оболонкою цивільних правових відносин і побутових угод; 2) шахрайства, що вчиняються під оболонкою адміністративних правових відносин; 3) шахрайства, що вчиняються під оболонкою господарських правових відносин. При цьому, шахрайствами, вчиненими під оболонкою цивільних правових відносин, визначені кримінальні правопорушення, при скоєнні яких злочинці для обману потерпілих використовують різні форми угод і домовленостей, врегульованих цивільним законодавством України. До шахрайств, вчинених під оболонкою адміністративних правових відносин, віднесено правопорушення, при скоєнні яких злочинці для заволодіння чужим майном або правом на нього використовують обман щодо наявності у них статусу суб’єкта владних повноважень або об’єму таких повноважень (статус службової особи). До шахрайств, вчинених під оболонкою господарських правовідносин, віднесено схеми обману, які реалізуються під час організації та здійснення господарської діяльності між різними суб’єктами господарювання [66, с. 3].

Втім, за останній час почали з’являтися роботи, в яких досліджуються питання боротьби та розслідування шахрайств в Інтернет просторі.

Так, основи методики розслідування кіберзлочинів були започатковані В. О. Голубєвимта О. Ю. Довженком. Вони охарактеризували історичні аспекти та сучасний стан методології боротьби з кіберзлочинністю; окреслили теоретичні основи методології розслідування кіберзлочинів відповідно до приписів чинного кримінального процесуального законодавства та з урахуванням віртуального характеру кіберзлочинності; провели дослідження типових слідчих ситуацій, що виникають при розслідуванні кіберзлочинів та розглянули тактику проведення окремих слідчих дій та їхні особливості, що визначаються «віддаленим», віртуальним характером діяння [44; 38].А вже А. І. Анапольська заклала базис для формування методики розслідування шахрайства у сфері функціонування електронних розрахунків [1].

О. М. Стрільців, В. В. Крижна та О. В. Максименко дослідили особливості розслідування кримінальних правопорушень, пов’язаних із розповсюдженням у мережі Інтернет забороненого контенту [175].

Не без уваги залишається й робота Т. В. Коршикової, яка присвятила своє дисертаційне дослідження комплексному дослідженню теоретичних, методичних і практичних проблем, пов’язаних з розслідуванням шахрайств, учинених з використанням електронно-обчислювальної техніки. Вченою розроблено алгоритм першочергових заходів, які здійснюють уповноважені підрозділи Національної поліції України в разі надходження інформації про шахрайство, вчинене з використанням ЕОТ, які об’єднано в блоки: з’ясування обставин шахрайства; внесення відомостей до ЄРДР; визначення напрямів встановлення IP-адрес, які використовувались ЕОТ з метою вчинення шахрайства; виявлення ЕОТ, які використовувались з метою вчинення шахрайства; фіксація причетності осіб до використання ЕОТ з метою вчинення шахрайства та отримання/неотримання коштів чи майна під час вчинення шахрайства; проведення СРД та НСРД. Вченою визначено

обставини, які підлягають встановленню під час розслідування шахрайств, учинених з використанням ЕОТ; розроблено наукові основи розслідування шахрайства, вчиненого з використанням ЕОТ, а також структуру криміналістичної характеристики. У її роботі визначено порядок і тактику огляду ЕОТ, а також інформації, що міститься в ній, з метою виявлення матеріальних та цифрових слідів, які можуть бути доказами у кримінальних провадженнях про вчинення шахрайства з використанням ЕОТ [81, с. 25].

Комплексною науковою розробкою із розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», є дисертація С. В. Самойлова «Розслідування шахрайств, учинених із використанням мережі «Інтернет»», в якій подано кримінально-правову характеристику та висвітлено деякі питання кваліфікації означеного виду злочинів. Автором наведено криміналістичну характеристику досліджуваних злочинів та детально розглянуто особливості початкового етапу розслідування шахрайств, учинених із використанням мережі «Інтернет». Окремо досліджено питання отримання інформації про правопорушення та прийняття рішення про початок кримінального провадження; наведено типові слідчі ситуації початкового етапу розслідування та розроблено відповідні їм слідчі версії і алгоритми їх перевірки. Вчений приділив увагу особливостям витребування інформації від установ та організацій під час розслідування шахрайств, учинених із використанням мережі «Інтернет» та дослідив особливості тактики проведення окремих слідчих дій під час розслідування зазначеного виду шахрайств та особливості застосування спеціальних знань різними суб’єктами [156; 157].

Проте, не дивлячись на вагомий вклад С. В. Самойлова у практику розслідування шахрайств, учинених із використанням мережі «Інтернет», слід констатувати, що робота виконана у 2014 р., що певною мірою втрачає деякі актуальні аспекти та не враховує сучасні реалії. До того ж, робота приділена загальній категорії шахрайств, вчинених через Інтернет і не охоплює докладно питання електронної комерції.

Найбільш ближчою до тематики нашого дослідження є дисертація С. В. Чучко «Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет», в якій автор вирішив низку завдань, зокрема: визначив особливості правового регулювання правовідносин у віртуальному просторі, що впливають на рівень вчинення шахрайства у мережі Інтернет; описав та систематизував типові способи шахрайства при купівлі-продажу товарів через мережу Інтернет;здійснив науковий аналіз криміналістичної характеристики шахрайства при купівлі-продажу товарів через мережу Інтернет; виявив проблемні питання початку досудового розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет; встановив особливості взаємодії різних органів у кримінальних провадженнях досліджуваної категорії;конкретизував організацію та тактику проведення окремих слідчих (розшукових) дій, спрямованих на отримання інформації з матеріальних та особистісних джерел;висвітлив особливості використання спеціальних знань під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет тощо [205].

Натомість, не дивлячись на те, що вказана дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням методики розслідування шахрайства, пов’язаного зі здійсненням угод купівлі-продажу товарів через мережу Інтернет, у якому сформульовано низку наукових положень і рекомендацій, що вирізняються науковою новизною, мають важливе теоретичне та практичне значення, ряд питань так і не знайшли свого висвітлення.

У цьому розрізі М. М. Єфімов справедливо наголошує, що проблема кібершахрайства розглядалась дослідниками на момент публікації їх робіт, і характеристика цього виду правопорушення щодня втрачає свою актуальність з огляду на стрімкий розвиток ІТ-технологій, і, як наслідок, удосконалюються способи, техніка, обізнаність шахраїв [55, с. 117].Підтримує цю позицію й С. В. Шапочка, що Інтернет-шахрайство зберігає сталу тенденцію до

еволюціонування, що спонукає до подальших наукових досліджень [210, с. 90].

Отже, значна кількість питань з розслідування шахрайств, пов'язаних з електронною комерцією, залишається не розглянутою. У практичній діяльності з цього напрямку існує коло аспектів, що потребують більш глибокого і всебічного вивчення. Такими питаннями є: правовий режим здійснення комерційних (торгівельних) операцій в Інтернеті та його вплив на формування криміналістичної характеристики комерційного інтернет-шахрайства; виявлення ознак шахрайства, пов'язаного із електронною комерцією; організація та тактика документування злочинної діяльності, пов'язаної з комерцією в інтернет-просторі; проведення тактичних операцій у провадженнях щодо шахрайства, пов'язаного з електронною комерцією. До того ж, невирішеними залишилася профілактична діяльність у таких провадженнях.

Таким чином, можна стверджувати, що сфера Інтернета та кримінальні правопорушення, які вчиняються у кіберпросторі, за різних часів становилась об'єктом пильної уваги вчених різних галузей знань. Одні приділяли увагу питанням законодавчого регулювання правовідносин, що регулюють правові та інформаційні відносини у мережі Інтернет. Інші зосереджували увагу на протидії таким кримінальним правопорушенням, а також питанням кримінально-правової кваліфікації та юридичній відповідальності за вчинення протиправних дій у кіберпросторі. Ряд наукових праць присвячений й питанням розслідування кримінальних правопорушень, вчинених у кіберпросторі. Натомість, перед наукою та практикою дотепер постає нагальна потреба у дослідженні питань, які потребують висвітлення та вирішення.

1.2. Концептуальні основи щодо формування криміналістичної характеристики шахрайства вінтернет-комерції

Криміналістична характеристика кримінальних правопорушень є основою для побудови методичних рекомендацій з розслідування певного виду або групи кримінальних правопорушень.

Разом із цим, існують суттєві суперечності у її визначенні, підходах до сутності, структури, методології формування та можливостей практичного використання. Так, на думку Р. Л. Степанюка, основною причиною розбіжностей у цих питаннях є неоднозначне розуміння різних рівнів криміналістичних характеристик, адже на сьогодні в науковій літературі фактично розглядається три значення криміналістичної характеристики злочинів: а) як назви криміналістичного вчення (окремої теорії); б) як частини окремої криміналістичної методики; в) як опису ознак окремого злочину [171, с. 173]. До того ж, як наголошує Є. Д. Лук'янчиков, криміналістична характеристика, як і кримінально-правова та кримінологічна характеристика, містить інформацію про злочин у цілому і його складові елементи (об'єкт та об'єктивну сторону), але, на відміну від них, по-перше, являє собою систему лише криміналістично значущих відомостей про ознаки злочину, а не будь-яких однакових для всіх видів злочинів, які в межах визначеного виду можуть сприяти його розкриттю. По-друге, відомості про ознаки елементів злочину описуються на якісно-кількісному рівні. Тобто встановлюються кореляційні закономірні взаємозв'язки як-от: що (дії, знаряддя, сліди й ін.) із чим пов'язано, яким саме чином, що за чим слідує, що та за допомогою чого може бути встановлено тощо. Практичне значення таких характеристик полягає в тому, що під час розслідування конкретного злочину зібрану про нього інформацію зіставляють зі системою узагальнених відомостей про злочини цього виду, які розслідували раніше (інформаційною моделлю). За збігом криміналістично значущих ознак злочину стає можливим з'ясувати, чим раніше характеризувалися поки що не відомі в цьому розслідуванні обставини [103, с. 108].

В. Ю. Шепітько розглядає криміналістичну характеристику як систему відомостей про певні види злочинів, ознаки суб'єкта злочину, його мотиви, предмет посягання, обстановку, злочинні способи, що мають значення для виявлення, розкриття цих діянь криміналістичними засобами і методами [92]. Водночас, моделлю системи зведених відомостей про криміналістично значимі ознаки виду, групи або конкретного злочину вважають криміналістичну характеристику злочину П. Д. Біленчук, В. К. Лисенко, Н. І. Клименко [91, с. 254].А вже А. Ф. Волобуєв додає, що в кожній приватній методиці сформувалася система знань, необхідних для розслідування певних злочинів, яка і позиціонується як криміналістична характеристика злочинів заданого виду. На думку вченого, криміналістична характеристика – це система відомостей (знань) про елементи механізму скоєння злочинів окремого виду або групи, в яких відображаються закономірні зв'язки між цими елементами і які використовуються для побудови і перевірки версій під час розслідування конкретних злочинів. У криміналістичній характеристиці повинні міститися відомості про такі елементи, як спосіб підготовки, скоєння і приховування злочину; місце і обстановка скоєння злочину; час скоєння злочину; знаряддя скоєння злочину; предмет посягання; особа потерпілого; особа злочинця [28, с. 24].

При цьому, як наголошує С. О. Сафронов, структура криміналістичної характеристики складна і неоднакова для всіх видів злочинів. Із погляду криміналістичної необхідності інтерес становлять виокремлення і вивчення таких видів зв'язків елементів криміналістичної характеристики, що мають характер закономірностей для цього виду злочинів, опираються на дані узагальнення практики [159, с. 17].

Виходячи з цього, можна сказати, що теоретичні положення та практичні рекомендації з розслідування шахрайства в інтернет-комерції можуть бути більш аргументованими у разі врахування особливостей правового режима, що регулює відносини між різноманітними суб'єктами, які беруть участь в укладанні дистанційних угод; характеристики цих

суб’єктів; предмета злочинного посягання; обстановки та умов, в яких вчиняється шахрайство в інтернет-комерції; способу шахрайських дій. Особливе криміналістичне значення має слідова інформація про подію.

Отже, можна виділити наступні елементи криміналістичної характеристики шахрайства в інтернет-комерції: спосіб вчинення шахрайства; слідова картина; особа шахрая; особа потерпілого; місце, час та обстановка в розрізі законодавчого регулювання комерційних правовідносин у мережі інтернет.

З’ясування початку і закінчення злочинних дій та їх тривалості у часі має велике значення для визначення часу безпосереднього закінчення шахрайства [127, с. 142]. Втім, час вчинення шахрайств з використання електронних технологій характеризується досить тривалою подією у часі. Злочинцю потрібен час для здійснення технічної підготовки до злочину, а також в деяких випадках отримати необхідну інформацію про потерпілого [151, с. 53].Отже, процес купівлі-продажу товарів та послуг через мережу Інтернет має особливості, що істотно відрізняються від традиційної торгівлі. Так, якщо шахрайство вчинене у залі торгівельного приміщення (центру, магазину тощо), місце вчинення цього злочину є очевидним. Інформацію про злочин та його учасників можна отримати шляхом огляду торгівельного приміщення, перегляду камер спостереження тощо. Через особистий контакт покупця з продавцем, вибір та замовлення товару покупцем, формується ряд ідеальних слідів, які відображаються в пам’яті потерпілих, свідків (охоронців, касирів, інших працівників). По-іншому складається ситуація у разі здійснення покупок через мережу Інтернет. Оскільки торгівельна точка є віртуальною, то і місце вчинення злочину носить віртуальний характер. Тобто, місцем вчинення шахрайства у широкому розумінні є інтернет-простір. З іншого боку покупець і продавець, домовляючись про укладання електронного правочину щодо купівлі-продажу товару, здійснюють таке віртуальне спілкування із матеріального середовища, маючи кожний свою ір-адресу [205].

З цього виходить, що кожний користувач мережі Інтернет і його комп’ютер діють автономно та формують єдину транснаціональну мережу, яка виходить за межі географічної концепції чітких кордонів. Поряд із цим, сервери переміщаються у фізичному просторі, тому може йтися мова про фізичні характеристики місця [3, с. 27]. Так, С. В. Самойлов до місць шахрайств, учинених із використанням мережі «Інтернет», відносить місцезнаходження: а) банкоматів (магазин, вулиця тощо); б) підключених до мережі «Інтернет» комп’ютерних систем (місце роботи, навчання, проживання, «Інтернет-кафе», зона вільного підключення до мережі «Інтернет» із використанням технології «Wi-Fi» - так звані «FrceWi-Fi-zone» romo); в) установ, де впроваджено системи розрахунків за допомогою пластикових кредитних карток тощо [156, с. 8].

Місце безпосереднього вчинення протиправного діяння (місце знаходження злочинця, засобів вчинення злочину) не співпадає з місцем знаходження потерпілого і настання наслідків злочину, що пов'язано з використанням електронних технічних засобів та мережі Інтернет. Зазвичай місцем вчинення інтернет-шахрайства можуть бути місця проживання, роботи або навчання злочинця. Тобто злочинець має можливість заволодіти майном потерпілого використовуючи лише технічні засоби, не маючи з ним особистого контакту, хоча, можуть здійснюватись телефонні дзвінки до потерпілого. Тому, можна відзначити, що місцезнаходження електронного технічного засобу і є місцем вчинення злочину [151, с. 53].

Безумовно час та місце вчинення шахрайства в інтернет-комерції мають важливе значення для встановлення істини у провадженні, між тим, є низка умов, які прямо пропорційно впливають на механізм вчинення цього кримінального правопорушення.

Загалом, вчинення шахрайства здійснюється в умовах складної взаємодії комплексу чинників економічного, політичного та соціального

характеру. Всі ці фактори впливають на систему і визначають її поведінку. У цьому розрізі можна виділити обстановку та умови, в яких можуть формуватися вплив на шахрайство: якщо в країні мінімальна заробітна плата є низькою, тоді населення країни більше схильне до шахрайських операцій ніж у суспільстві, в якому вища заробітна плата;в країні в якій велика кількість населення має дохід нижче валового доходу схильність до здійснення шахрайських операцій зростає;коли в країні йде поширення корупційної складової, то схильність до здійснення шахрайських операцій буде збільшуватися;коли суспільство не має право вибору на бажану роботу, виробництво товарів, різних витрат та інвестицій, тоді в населення виникає схильність до здійснення шахрайства більше ніж в суспільстві, яке має вільні економічні права;країна в якій економічний розвиток не на високому рівні, купівельна спроможність населення низька, то можливе виникнення шахрайських операцій;висока схильність до виникнення шахрайства буде в регіонах, в яких буде збільшуватися рівень цін на товари та послуги, які купує населення для невиробничого споживання, а купівельна спроможність населення буде залишатися на низькому рівні. Вибір цих факторів обумовлений тим, що різні макроекономічні дії в країні спричиняють формування в населенні схильності до здійснення шахрайства [72, с. 106].

Не без уваги слід залишити й предмет шахрайського посягання. В науково-практичних коментарях до кримінального кодексу України зазначається, що предметом абсолютної більшості кримінальних правопорушень проти власності є майно, тобтопредмети матеріального світу, яким притаманні специфічні ознаки фізичного, економічного та юридичного характеру, що в цілому утворюють три підгрупи:а) речі;б) гроші (у готівковій чи безготівковій формі);в) цінні папери (акції, облігації, векселі, а також легітимаційні знаки, які виконують роль грошового еквівалента та є оборотоздатними) [116, с. 106].

Натомість, слід зауважити, що у криміналістичній літературі окрім терміну «предмет злочинного поягання» зустрічаються ще й такий

термінологічний зворот, як «об'єкт злочинного посягання». Виходячи з того, що етимологічне значення слова «посягання» – це дія за значенням «посягати», та враховуючи, що криміналістику цікавить злочине діяння як реальна подія в динаміці, а не його теоретикозаконодавча конструкція, криміналісти і ввели криміналістичний термін «предмет посягання», намагаючись саме таким чином відобразити криміналістичний аспект дослідження злочину. Вживання саме його в криміналістичній літературі на думку ряду науковців є найбільш адекватним [120, с. 257].

З цього приводу Н. В. Павлова повідомляє, що у провадженнях щодо шахрайства предметом злочинного посягання може виступати як майно, так і право на майно. Проте, для того, щоб визнати право власності на майно предметом шахрайства, слід проаналізувати підстави набуття такого права та підстави володіння таким правом його власником на момент посягання. Адже дії з набуття права власності повинні бути правомірними та добросовісними та випливати із правочинів [129, с. 59].

Як показав аналіз кримінальних проваджень щодо шахрайства в інтернет-комерції, 87 % випадків предметом посягання виступає все ж таки не право на майно, а саме майно (речі, гроші та цінні папери).

В контексті даної проблематики В. П. Чайковська звертає увагу, якщо раніше електронна комерція була представлена переважно побутовою/цифровою технікою і книгами, то у подальшому спостерігається перерозподіл категорій. У 2016 році найбільш зростаюча онлайн-категорія товарів – одяг, на другому місці – будівництво, а техніка – на третьому плані. У сегмент електронної комерції заходять все нові категорії, користувачі все частіше купують через Інтернет товари, які раніше віддавали перевагу шукати в офлайні. За рахунок цього зростає весь ринок e-commerce в Україні [195, с. 45].

Втім, починаючи з 2019 року нашу країну охопила пандемія Covid-2019, внаслідок чого об'єктами комерциалізаії в мережі Інтернет стали ліки від цієї хвороби, маски, апарати штучного дихання тощо. Відповідно,

дані об’єкти стали фігурувати й у провадженнях щодо шахрайства в інтернет-комерції.

На момент повномасштабного вторгнення рф на територію України 24 лютого 2021 року електронна комерція пережила спочатку шокове падіння, потім сплеск попиту на окремі категорії товарів і нарешті певну стабілізацію після масового переміщення людей, релокації складів та виробництв. Облаштування людей на новому місці або повернення їх додому поступово повертає продажі в інтернеті до зростання. Проте попит змінився. Прихильність до брендів у споживачів дуже низька – купують те, що є. Динаміку зростання зберігають категорії, які закривають базові потреби: продукти харчування, сигарети, медикаменти, взуття та одяг, гігієнічні та господарчі товари, товари для тварин. По мірі відновлення країни у топі продажів опиняться будматеріали, товари для дому, техніка та електроніка [33].

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

Так, слідчі та оперативники Солом’янського управління поліції спільно із співробітниками управління протидії кіберзлочинам міста Києва та за процесуального керівництва Солом’янської окружної прокуратури затримали чоловіка, який розміщував у мережі Інтернет оголошення про продаж неіснуючих бронежилетів і тактичних плитоносок [185].І таких випадків велика кількість. Користуючись ситуацією із дефіцитом пального, зловмисники створюють сайти для «продажу» неіснуючих талонів до різних мереж АЗС. Так, користувачам пропонувалося придбати паливні картки, що не лише дозволяли заправитися без обмежень за кількістю літрів, а й за цінами нижче на 30-40% від реальної вартості палива. Для реклами створених вебсайтів фігурант використовував тематичні групи у

месенджерах. Отримавши повну оплату за талони, чоловік припиняв зв'язок із клієнтами. Загальна сума збитків, завданих потерпілим, сягає щонайменше 200 тисяч гривень [76].

Слід сказати, що останнім часом широкого поширення і популяризації набуло використання децентралізованих віртуальних криптовалют: Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin тощо. Нерегульована сфера обігу віртуальних валют стала користуватися великою популярністю також серед організованих злочинних угруповань, що приймають оплату за свої послуги у віртуальній валюті, використовуючи альтернативний "темний" Інтернет – DarkNet, що функціонує на основі системи The Onion Router [231, с. 64; 209, с. 63].

Натомість, абсолютно новим поглядом і певною проблемою для кваліфікації шахрайств в частині визначення предмету кримінального правопорушення, може стати невизначеність статусу криптовалют. Так, останнім часом в комерційних секторах України все частіше при купівлі-продажу використовується «віртуальна валюта» або криптовалюта. На сьогодні офіційно в Україні криптовалюта не визнана платіжним засобом, вона не дозволена законом, але і заборони на неї немає. З тієї причини, що криптовалюта не заборонена в законі, продавці й покупці знайшли можливість використовувати її в правочинах [160, с. 64; 12, с. 51].

Натомість, слід зауважити, що платежі криптовалютами на зразок: bitcoin, litecoin, tron, XRP і інші не врегульовані практично в жодній країні світу. Криптовалюта за чинним законодавством України не належать ні до електронних грошей, ні до коштів, ні до цінних паперів. Відповідно, при розрахунках криптовалютами РРО не застосовуються і чек покупцеві не видається.Зважаючи на сумнівний правовий статус криптовалют, розрахунки криптовалютами не можна вважати офіційними та прозорими [24].

Отже, предметом посягань у провадженнях щодо шахрайств в інтернет-комерції є: гроші, різноманітні товари побутового призначення,

предмети, які мають стратегічне призначення (бронежилети, каски, воєнна техніка) тощо.

Серед елементів криміналістичної характеристики домінуюче місце посідає спосіб вчинення кримінального правопорушення.

Спосіб скоєння злочину дає найбільший обсяг криміналістичної інформації, який в подальшому допомагає слідчому, прокурору, суду чи іншим посадовим особам правоохоронних органів визначити найбільш ефективні методи, спрямовані на розкриття та розслідування злочину, дасть змогу слідчому висунути необхідні версії та ініціювати проведення необхідних слідчих (розшукових) дій, визначити правильний порядок та послідовність їх проведення [88, с. 370].

Не дивлячись на безупинні дискусії з приводу поняття та структури способу вчинення кримінального правопорушення, ми вважаємо доцільним розглядати спосіб вчинення шахрайств в інтернет-комерції як комплекс дій з підготовки, безпосереднього скоєння та приховування злочинних дій.

У розрізі цієї проблематики, обґрунтовуючи повноструктурність способу, В. В. Білоус влучно зазначає, що під час готування до злочину, при вчиненні злочину і після нього особа керується логікою досягнення злочинного результату та уникнення відповідальності. Злочинець, маючи наміри приховати злочин, ретельно обмірковує спосіб його вчинення з тим, щоб надійно приховати сліди злочину. Крім вибору місця і часу вчинення злочину, підготовка до нього включає визначення: а) способу вчинення злочину; б) знарядь злочину; в) способу приховування (дійсного приховування і притворної поведінки, що відображає позицію, обрану злочинцем) г) способу приховування слідів. Таким чином, злочинець уявно формулює модель майбутньої події, реальне втілення якої буде залежати від ситуації, що об’єктивно складеться. Моделювання включає і варіанти зміни намірів і злочинної поведінки у випадку, якщо обрана схема не може бути реалізована [17, с. 40].

Як показав аналіз кримінальних проваджень щодо шахрайств в інтернет-комерції, без підготовки не вчиняється жодне таке кримінальне правопорушення. Цей факт можна пояснити складним механізмом здійснення правочинів у дистанційному варіанті.

Наприклад, інформацію про товари та послуги «потерпілий» може отримати тільки із соціальних мереж, а для цього шахраям слід продумати різноманітні варіанти із створення сайтів, розміщення інформації в соціальних мережах, підтримання рекламування товарів та послуг тощо з метою зацікавлення населення.

Своєю чергою, створення сайту зазвичай включає три основні етапи робіт: розробка дизайну сайта, верстання його веб-сторінок і його програмування. Для роботи сайта необхідно зареєструвати доменне ім’я (головна складова адреси в мережі Інтернет) і сплатити за хостинг (послуги з розміщення сайта в мережі – на інтернетному сервері) [27, с. 8].

Разом з тим, процес створення Інтернет-магазину взагалі умовно розділяється на 6 етапів. На першому етапі створення Інтернет-магазину підприємцю необхідно визначити: що він буде продавати, наскільки цей товар підходить для торгівлі через Інтернет. Ідеальний об'єкт для Інтернет-торгівлі – це стандартні не швидкопсувні товари з гарантованими споживчими властивостями. Не будь-який товар може бути реалізований через мережу Інтернет, так певні товарні категорії мають специфічні обмеження для торгівлі в Інтернеті: одяг і взуття вимагають приміряння, ліки й продукти - термінової доставки й т.п. На другому етапі здійснюється оцінка конкурентів – аналіз сайтів, що пропонують такі ж або аналогічні товари або послуги. На третьому етапі визначається, якими функціями повинен володіти Інтернет-магазин. На четвертому етапі здійснюється розробка технічного завдання на створення Інтернет-магазину. Цей процес повинні здійснювати професіонали в області інформаційних технологій (IT), добре знайомі зі специфікою діяльності компанії. Технічне завдання повинне описувати (визначати) структуру Інтернет – магазину, його дизайн, принципи роботи та

розташування інформації. На п'ятому етапі здійснюється вибір необхідного програмного забезпечення для реалізації Інтернет-магазину та безпосередньо сама реалізація проекту. На шостому етапі відбувається розміщення сайту магазину у мережі Інтернеті. Існуючі варіанти розміщення сайту: на власному сервері, при цьому він або розташовується у комп'ютерній мережі провайдера за відповідну абонентську плату, або підключається до провайдера за виділеною лінією; на устаткуванні провайдера (віртуальний сервер), у цьому випадку у провайдера орендується дисковий простір (хостінг) [194, с. 39].

Виходячи з цього, можна виділити наступні підготовчі дії щодо шахрайства в інтернет-комерції.

Зокрема, підготовчі дії шахраїв можуть полягати у: обранні товару, що пропонуватиметься для продажу, визначенні його характеристик, створенні портфоліо;обранні доменного ім’я (адреси сайту магазину в Інтернеті);реєстрації хостингу під сайт (місця на віддаленому сервері, який відводиться провайдером послуг); пошуку постачальників, закупівлі товару або створенні його особисто тощо (у разі, якщо є намір отримати гроші за фальсифікований товар під виглядом «брендового»); створенні веб-дизайну танеобхідних інформаційних та тематичних сторінок, наповненні інтернет-магазину товарами, рекламуванні продукції; обранні способу здійснення розрахунків (з використанням платіжних інструментів, електронних грошей, шляхом переказу коштів або оплати готівкою тощо); обранні способу доставки (у разі, якщо не йдеться про отримання грошей без наміру надіслати товар) [206; 54].

При цьому, способи підготовки до шахрайства, що вчиняється від імені вигаданих осіб, мають дещо спрощений вигляд: визначення найменування товару, що пропонуватиметься для продажу, створення його характеристик та отримання презентабельних фотографій; реєстрація та створення облікового запису особи в інформаційній телекомунікаційній системі під вигаданими анкетними даними; розміщення даних про товар; створення рівня довіри у покупців шляхом здійснення успішних цивільно-правових дистанційних угод

та заповнення шкали позитивних оцінок; створення «окремої» електронної адреси для здійснення переписки із потенційним споживачем; придбання «окремого» телефонного номеру для здійснення переговорів із потенційним споживачем; обрання способу здійснення розрахунків; реєстрація «електронних гаманців» у відповідних сервісах або отримання платіжної картки для перерахування грошей тощо [206].

Отже, шахрайство в інтернет-комерції може мати достатньо широкі межі. Так, протиправні дії можуть початися з розміщення оголошення про продаж товарів та послуг, створення фіктивних сайтів, крадіжки персональних даних тощо, а закінчитися отриманням грошей від потерпілих в обмін на «не існуючі товари» чи «не існуючі послуги». Залежно від кінцевої мети, дії можуть припинятися на певному етапі.

Як показує практика, шахраї не тільки ретельно здійснюють підготовку до злочину даної категорії, але й заздалегідь планують дії з приховування.

Наведемо приклад. Так, у ході розслідування правоохоронці з'ясували, що 21-річний мешканець Вознесенського району розміщував оголошення на інтернет-майданчиках про продаж квадроциклів, мотоциклів і мотоблоків та нібито продавав за попередньої або повної оплати за товар, після чого зникав. Для конспірування своєї злочинної діяльності шахрай застосовував широкий спектр засобів анонімізації в мережі, створив більше 100 фейкових акаунтів на інтернет-платформах, постійно змінював засоби зв'язку, а для заволодіння коштами використовував банківські картки, оформлені на підставних осіб [114].

Загалом, способами приховування шахрайства в інтернет-комерції можна назвати: виготовлення та використання фіктивних документів при реєстрації на сайті (22% випадків); маскування злочину під легальні цивільно-правові угоди (24%); знищення електронних документів, які 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 %) тощо.

О. Л. Андронік та А. В. Воронін зауважують, що часто покупці зіштовхуються з невірно вказаною інформацією про товар, з незадовільною якістю придбаного товару чи послуг; продавець не дотримується термінів виконання доставки замовлення чи відмовляється виконувати повернення товару та коштів. Разом з тим, купуючи на маркетплейсах покупці часто ризикують зіткнутися з різними шахрайськими схемами. Наприклад, виконують передплату на картку і не отримують товар, недоброчесні продавці можуть попросити перейти з спілкування в особистому кабінеті у будь-які інші месенджери (Viber, Skype, Telegram, WhatsApp тощо), де пізніше надсилають покупцеві посилання на фішинговий сайт. Тому важливо перевіряти відповідність URL оригінальним сайтах та уникати спілкування не в особистих кабінетах [2, с. 126].

С. В. Шапочка акцентує на поширенні таких його видів: у сфері дистанційного банківського обслуговування, з електронними платіжними системами і системами експрес-оплати товарів і послуг (жебрацтво, фейкові банки, біржі праці, електронні віртуальні гаманці, фейкові листи від чужого імені, Інтернет-аукціони, Інтернет-лотереї, віртуальні казино й тоталізатори) [209, с. 63].Втім, як на наш погляд, найбільш широкий спектр дій щодо шахрайства в інтернет-комерції було розглянуто С. В. Чучко, який наводить у своїй дисертації безліч шахрайських схем щодо заволодіння грошима громадян, які здійснюють угоди через мережу Інтернет. Покладаючи в основу такий критерій класифікації, як зміст вчинюваних дій, всі варіанти шахрайських дій при купівлі-продажу товарів через мережу Інтернет, можна класифікувати у такий спосіб: розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його вартості; розміщення фейкової інформації про продаж товару за умов накладного платежу з подальшим отриманням частини його вартості на платіжну карту (передоплати); створення сайтівмагазинів у мережі Інтернет

або їх копій, що діють за принципом фірм-одноденок; кібер-втручання в обліковий запис сумлінного продавця, рівень довіри якого відповідає потребам споживачів, і здійснення шахрайських угод від його імені; отримання грошей за лот, виставлений на інтернет-аукціоні, від декількох покупців відразу; отримання грошей за фальсифікований чи заздалегідь зіпсований товар; отримання грошей за товар, що повинен складатися з великої кількості вузлів і комплектуючих без надання всієї складової (за умов, якщо це заздалегідь сплановано); шахрайські дії від імені несправжнього «покупця» шляхом отримання ним інформації про номер карткового рахунку, персональні дані та номер мобільного телефону продавця «під легендою» необхідності перерахування грошей із подальшим зняттям з рахунку всіх коштів; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати) [205, с. 92].

За даними соц. опитування, більше половини випадків шахрайства (54%) склали продажу неіснуючих товарів за передоплатою. На другому місці (28%) виявилися фішингові атаки, коли в месенджерах користувачам надсилали шкідливі посилання на підроблену платіжну форму. На третьому місці (11%) - шахрайства з відправкою фейковий скріншотів / квитанцій про оплату товару. За даними OLX, схема з підставним кур'єром(коли приїжджає таксист і шахрай-покупець переконує швидко віддати йому товар, обіцяючи зарахування коштів на рахунок продавця*)* вже не так популярна. На неї попалися всього 7% опитаних. 14% жертв втрачають свої кошти в результаті фішингових атак шахраїв під час онлайн-шопінгу. У 83% випадків сторонні посилання на шкідливі сайти надходять прямо в месенджери (Telegram, Viber, WhatsApp). Ще 6% жертв отримали фішингові посилання в вигляді SMS [186].

Хотілось би зазначити, що одним із найпотужніших поштовхів до розвитку шахрайств у мережі Інтернет за останні три роки стала всесвітня пандемія COVID-19 та війна з рф[55].

Відсутність роботи у період карантину та війни, перехід на онлайн-торгівлю, намагання людей уникати фізичних контактів спровокували реальний ринок товарів та послуг дуже швидко зануритись у мережеві торгові відносини. Фактично люди були змушені погодитись із сучасними правилами життя і, не маючи достатнього досвіду користування Інтернетом, будучи недостатньо обізнаними у питаннях приватності та інформаційної безпеки у всесвітній мережі, дуже легко перетворились на жертв кібершахраїв [55, с. 117].

Натомість, із початком воєнного стану з'явилися й нові способи недобросовісних дій, у тому числі й через мережу Інтернет.

Одна з найпоширеніших схем кібершахрайства, від якої постраждали тисячі українців (особливо на сході нашої країни) – імітація перевезення до безпечних міст та допомога в розміщенні. Злодії розміщують в мережі інтернет оголошення, пропонуючи усім бажаючим швидко та безпечно виїхати до заходу України чи навіть за кордон. У ході спілкування шахраї намагаються виманити передоплату за свої послуги, посилаючись на небезпеку, необхідність резервування місць та інше. Зазвичай за свої «послуги» зловмисники вимагають від 500 до 1000 гривень авансу з особи. Отримавши передоплату, шахраї зникають та перестають виходити на зв'язок[212].Ще одна схема шахрайств, які здобули поширення з початком воєнних дій – діяльність фейкових благодійних та волонтерських організацій. Під виглядом збору грошей на благодійність аферисти створюють фіктивні сайти, сторінки в соціальних мережах, канали в телеграм та привласнюють кошти громадян. Приклад реальної історії шахрайства на псевдо благодійності: на Вінниччині 31-річний громадянин України збирав в Інтернеті гроші нібито на обладнання для військового шпиталю. За час своєї діяльності шахраю вдалося виманити 53 благодійні внески від небайдужих людей, проте ці кошти були витрачені аферистом на власні потреби. Для своєї шахрайської діяльності зловмисник створив фейкові сторінки в соціальних

мережах, де розміщував справжні дописи про збір грошей, однак в оголошеннях змінював банківські реквізити на власні [212].

Як ми вже раніше зазначали, шахрайські дії можуть бути пов’язані з закупівлею товарів для військових. Наші захисники, які задіяні в зоні активних бойових дій потребують допомоги у вигляді якісної амуніції, бронежилетів, рукавиць, наколінників, розвантажувальних жилетів, лікарських засобів. У мережі інтернет існує безліч оголошень щодо продажу товарів для потреб армії. На жаль, серед продавців трапляються аферисти. Схема роботи шахраїв досить проста – в інтернеті розміщується оголошення щодо продажу товарів, які користуються попитом. Посилаючись на небезпеку, зловмисник намагається витягнути передоплату, після отримання якої зникає [212; 74].

Співробітники Департаменту кіберполіції викривають все частіше шахрайство, пов’язане із на евакуаційними перевезеннями. Так, потерпілі намагалися виїхати з регіонів, де зараз тривають активні бої, зокрема з Маріуполя. Чоловік у Telegram-каналах публікував оголошення про організацію пасажирських перевезень. Від клієнтів він вимагав передплату від 500 до 3000 гривень на банківську картку. У такий спосіб фігурант ошукав щонайменше 15 людей [73; 145].

Виходячи з цього, можна побачити, що в основу шахрайських дій можуть покладатися не тільки дії щодо пропонування товарів, а й і послуг, за які потерпілі також готові сплачувати значні кошти.

Так, наприклад, троє фігурантів, мешканці Новомосковська та Запоріжжя, створювали у соцмережах сторінки, де пропонували виготовлення під замовлення меблів для салонів краси. Головною умовою була передплата. Однак, отримавши гроші клієнтів, зловмисники їх блокували та не виходили на зв'язок. Для протиправної діяльності вони постійно створювали нові сторінки, адже ошукані громадяни надсилали скарги для блокування фейкових магазинів. Загальна аудиторія їхніх акаунтів становила близько 100 тисяч підписників[75].

У цьому розрізі, Р. Ю. Царьов слушно наголошує, що всі види інформаційних послуг, які існують у традиційній економіці, досить легко інтегруються у мережі Інтернет. Практично всі послуги, які, так чи інакше пов'язані з передачею інформації, можна здійснювати через Інтернет: юридичні, консалтингові, фінансові, туристичні, медичні, психологічні та інші. Крім інформаційних послуг в Інтернеті надаються і комунікативні послуги: електронна пошта, Інтернет-телефонія, відео-конференції та ін. Туроператори мають свої web-вузли оптової торгівлі туристичними послугами, за допомогою корпоративних систем бронювання КСБ пропонують турпродукти туристичним агентствам. Онлайнова система резервування (бронювання) турів через Інтернет дозволяє турагентствам не тільки одержати повну інформацію про тур-продукти, які пропонуються, включаючи ціни, дати вильоту, категорії готелів та інші необхідні відомості, але й бронювати обраний тур у режимі реального часу. Ефективність GDS різко знизилася у зв'язку з появою Інтернет технологій, що дозволяють пропонувати кінцевим покупцям придбання послуг на пряму, безпосередньо в системах авіакомпаній та в інших постачальників туристичних послуг. Деякі авіакомпанії стимулюють Інтернет-клієнтів використати електронні квитки, пропонуючи безкоштовні послуги й бонуси при їхньому оформленні. Оскільки клієнти, що діють через Інтернет, бронюють квитки, вибирають місця й повідомляють інформацію про пластикові карти безпосередньо у Інтернеті, одержання ними електронного квитка замість паперового виглядає цілком природно. На сайтах страхових компаній відвідувач може придбати страховий поліс безпосередньо через Інтернет, порівняти ціни. Оплативши поліс, клієнт одержує його поштою або в електронній формі з електронним цифровим підписом страхової компанії. Клієнти Інтернет-страховника можуть заходити на персоніфіковані сторінки для перевірки дії страхового договору, для внесення чергової страхової премії або подачі заяви про страховий випадок [195, с. 48].

Щодо слідів, Л. П. Паламарчук слушно зазначає, що через специфіку таких кримінальних правопорушень, сліди при розслідуванні злочинів у сфері використання комп'ютерних технологій рідко виявляються у змінах зовнішнього середовища [132, с. 38]. При цьому, вони в основному не розглядаються сучасною трасологією, оскільки в більшості випадків носять інформаційний характер, тобто є тими або іншими змінами в комп’ютерній інформації, що виражається у формі її блокування, копіювання, модифікації, знищення. Скоєння особою протиправних дій, пов’язаних з використанням комп’ютерних технологій спричиняє виникнення певної кількості слідів у тому числі і специфічних, притаманних лише зазначеній категорії злочинів. Використання цих інформаційних даних при розслідуванні злочинів є необхідною умовою забезпечення всебічного, повного й об’єктивного дослідження обставин справи [48, с. 263].

Специфіка механізму утворення інформаційних слідів визначається кіберпростором, тобто слідоутворюючим об'єктом, яким виступає програмно-технічний засіб, а слідосприймаючим об'єктом – комп'ютерною інформацією[151, с. 53].

Сліди можуть міститися й у історії голосових повідомленнях та і відеодзвінках (відеододатки Skype, GoogleHangouts, Zoom тощо). Втім, найцінніша інформація криється у доменній адресі (Ip), що дозволяє встановити місцезнаходження точки доступу до комп’ютера, з якого здійснювалося спілкування [205, с. 74].

Матеріальні сліди також можуть залишатися на обчислювальній техніці (сліди від пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо), а також на магнітних носіях і оптичних дисках. На його думку, до окремого типу належать інформаційні сліди, що утворюються внаслідок впливу на комп’ютерну інформацію (шляхом знищення, перекручення). Вони залишаються на магнітних носіях інформації і пов’язані зі змінами, які відбулися у самій інформації порівняно з початковим її станом. Також до інформаційних слідів належать наслідки роботи антивірусних і тестових

програм, які можуть бути виявлені під час вивчення комп'ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм та програмного забезпечення [133, с. 8].

Як показав аналіз судово-слідчої практики та опитування респондентів у провадженнях щодо шахрайства в інтернете-комерції, сліди можуть залишатися: в пам'яті телефону (78 %); на сім-картці (48 %); в комп'ютері (81 %); на сервері мобільного оператора (18 %); на сервері інтернет-провайдера (17 %); на флешці, зовнішньому вінчестері (38 %); в пам'яті системи відео спостереження (зал інтернет-кафе, фойє банку, територія біля банкомату тощо) (31 %); в пам'яті електронного журналу банкомату (терміналу) (67%); в історії платіжних переказів через банківську систему (78 %); на квитанціях та роздруківках про електронні банківські платежі (51 %); на банківських картках(37 %); сліди папілярних ліній на засобах комп'ютерної техніки, клавіатурі терміналу (38 %) тощо.

Для визначення осіб, які потенційно можуть мати причетність до шахрайства в інтернет-комерції, слід наголосити, що у рамках електронного бізнесу постійно відбувається взаємодія між чотирма постійними його суб'єктами: клієнти – це продавці та споживачі товарів або послуг, які вони можуть придбати; бізнес-організації – це будь-яке підприємство, яке здійснює повністю або частково свою діяльність за допомогою інформаційних мереж, тобто займається електронною комерцією; фінансові установи – це організації, які надають послуги, пов'язані з пересування фінансових потоків, насамперед – це банки; держава – визначає правила ведення електронного бізнесу та здійснює загальне його регулювання [110].

Перша група включає в себе осіб, які є споживачами послуг банків чи фінансово-кредитних компаній, тобто шахраї від першої сторони – безпосередні учасники. Шахрайство починається тоді, коли клієнт не має наміру в подальшому виконати зобов'язання щодо дистанційної угоди. Разом з тим, другу групу складають шахрайства від третьої сторони, тобто від осіб, які не пов'язані ні з провайдером фінансово-кредитних послуг, ні з їх

клієнтами. Таке шахрайство здійснюється сторонніми особами шляхом використання фальшивих ідентифікаційних документів, без відома особи, чия особа використовується для здійснення шахрайства. Сюди ж відноситься шахрайська діяльність, пов'язана з незаконним отриманням конфіденційних даних клієнтів банків, ПІН-кодів та CVV2-кодів банківських карток, логінів та паролів від інтернет-банкінгу, заволодівання мобільними фінансовими номерами клієнтів, за якими здійснюється аутентифікація, тощо. У випадку шахрайства від третьої сторони вкрай складно визначити особу самого шахрая, відслідкувати його місцезнаходження. Тому такі види шахрайств є найбільш популярними, оскільки зловмисники часто залишаються не спійманими. Що стосується шахрайств від третьої сторони, то вони здійснюються переважно над поточними рахунками клієнтів (Current Accounts). Також популярними є шахрайства з банківськими картками (Cards) та ощадними рахунками (Saving Accounts). Тобто шахраї можуть отримати доступ до рахунку клієнта шляхом застосування методів соціальної інженерії, що є найбільш популярним способом шахрайства. Також можливі випадки, коли ідентифікаційні дані клієнта викрадаються з бази даних банку. Відомі випадки, коли банківські працівники продавали бази даних стороннім особам, за рахунок чого шахраї отримували доступ до даних клієнтів. Тут певну роль відіграє нехтування клієнтами елементарних правил безпеки власних конфіденційних даних, їх необережність при здійсненні розрахункових операцій та довірливість [219; 72; 2].

До того ж, в інформаційному просторі і процесах діє безліч посередників – провайдерів або операторів в системі мережі Інтернет та інших суб'єктів, що надають різноманітні види послуг. Зокрема, суб'єктами інтернет-відносинє: 1) оператори та провайдери телекомунікацій, які забезпечують функціонування мережі Інтернет як інформаційної системи; 2) виробники, власники і розповсюджувачі інформації та інформаційних ресурсів, які створюють інформаційне наповнення мережі Інтернет; 3) суб'єкти, які надають специфічні послуги з укладання електронних

(мережевих) угод (договорів) за допомогою мережі Інтернет, тобто все те, що охоплюється терміном «електронна комерція (торгівля)» та ін. Натомість, не так часто, але мають місце випадки, коли вказані суб'єкти надають пряму або опосередковану допомогу злочинцям у вчиненні шахрайства [206, с. 236; 205].

Отже, можна надати класифікацію осіб, які вчиняють шахрайство в інтернет-комерції:

- 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.

У відповідній більшості метою вчинення таких шахрайств є бажання отримати «безоплатні» надходження, що зумовлено відповідним стилем життя шахраїв, який заснований на гіпертрофованих потребах. Особі такого злочинця властива усталеність корисного спрямування, тобто ступінь стійкості психологічної готовності до вчинення злочинів, що пов'язано з протиправним збагаченням. Професіоналізм зазначених злочинців полягає в тому, що вони вміло маскують свій корисливий мотив, використовуючи для цього найрізноманітніші способи, наприклад, здійснюють навмисне або фіктивне банкрутство [62, с. 136-137].

Морально-психологічна характеристикаособи представляє собою синтез внутрішніх якостей особистості та її деяких проявів. Вона включає в себе психологічні особливості, інтереси, потреби, соціальні установки й орієнтації, моральні якості, звички особи. Центральним елементом у системі морально-психологічних ознак винної особи є мотиваційна спрямованість дій злочинця, тобто встановлення мотивів вчинення злочину [200, с. 97].

Саме низький рівень принципів і норм поведінки людини в суспільстві, на роботі, у побуті призводить до вчинення шахрайства. Люди втратили здатність соромитись за аморальну поведінку, переживати почуття провини за вчинене, відчувати докори сумління за протиправні вчинки, тому відбувається кількісне і якісне зростання шахрайства, що особливо помітно на фоні економічних кризових явищ [110].

Основні тенденції щодо розвитку кіберзлочинності та злочинної діяльності Інтернет шахраїв продовжують зберігатися. Відбувається консолідація ІТ-злочинців у групи, з подальшим їх укрупненням до злочинних угруповань, злочинних організацій, що діють на постійній основі – «професійна кіберзлочинність». Також, має місце швидке налагодження та зміцнення зв'язків між злочинними угрупованнями, що дає змогу забезпечити оперативний обмін інформацією щодо об'єктів шахрайського посягання шляхом надання у користування бот-мереж, здійснення обміну прийомами та способами вчинення злочинів, способами переведення електронних коштів у готівку тощо [209, с. 63].

Цей факт підтвердився й у ході аналізу судово-слідчої практики. Так, останні роки шахрайство, пов'язане із елетронною комерцією, все частіше стає об'єктом злочинної діяльності організованих злочинних угруповань. Іноді злочинці діють на транснаціональному рівні.

Наведемо приклад. Протягом 2019-2022 рр. злочинне угруповання використовувало скомпрометовані дані клієнтів іноземних банків для розрахунків в онлайн-магазинах. Куплені товари фігуранти перепродавали та одержували «прибутки». Транснаціональна злочинна група упродовж трьох років діяла на території ЄС та України, за цей період організаторам вдалося заволодіти грошовими коштами громадян ЄС на суму понад 600 тис. євро. [192].

Потерпілими від шахрайства, пов'язаного із купівлею-продажем товарів через мережу Інтернет, можуть виступати будь-які фізичні особи, підприємці, інші споживачі товарів та послуг. Втім, бажання швидкого придбання товару

при мінімальних витратах, небажання прискіпливо та ретельно перевіряти історію постачальників товару та незахищеність конфіденційної інформації про себе роблять таких осіб жертвами шахраїв [205]. До того ж, з огляду на значні прогалини у правовому регулюванні інтернет-торгівлі, пересічний споживач має досить обмаль знань щодо функціонування Інтернет-магазину та можливостей захисту своїх інтересів у разі їх порушення при купівлі товарів через такий магазин [53; 27].

Так, шахраї знаходили оголошення щодо продажу товарів на тематичних платформах та для обговорення деталей писали продавцям у сторонні месенджери. Туди зловмисники надсилали фішингові посилання нібито про інтернет-оплату. Коли продавці переходили за посиланням та вводили дані банківської карти, ці відомості одразу ставали відомі шахраям. Далі відбувалися злочинні операції з їх рахунками [184].

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.

Висновки до розділу 1

1. Кримінальні правопорушення, 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 протиправних 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.

2. Теоретичні положення і практичні рекомендації з розслідування шахрайства в інтернет-комерції 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.

3. Обстановку шахрайства в інтернет-комерції необхідно розглядати, з урахуванням просторово-часових характеристик, а також умов складної взаємодії комплексу чинників економічного, політичного та соціального характеру.

4. Предметом шахрайства в інтернет-комерції 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 шахрайства в інтернет-комерції в якості предмету посягання стали фігурувати ліки від цієї хвороби, маски, апарати штучного дихання, а під час воєнного стану збільшуються випадки, коли предметом шахрайства є речі, необхідні для несення служби у зонах бойових дій (воєнний одяг, бронежилети, каски, військове обладнання, генератори тощо).

5. Основними діями, до яких вдаються шахраї при підготовці й вчиненні шахрайства в інтернет-комерції, є: 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.

6. 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 тощо).

7. Сформовано типовий портрет особи шахраяз 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.

8. 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 ВІНТЕРНЕТ-КОМЕРЦІЇ

2.1. Оцінка первинної інформації на початку кримінального провадження

Розслідування слід починати з аналізу вихідної інформації, що надійшла до слідчого. Внаслідок такого аналізу особа, яка приймає рішення щодо відкриття кримінального провадження та внесення інформації до ЄРДР, повинна провести належну оцінку, осмислити наявну інформацію, та зрозуміти, що в ній дійсно містяться ознаки кримінального правопорушення, зокрема, шахрайства в інтернет-комерції, та є підстави до початку досудового розслідування [181].

Оцінюючи ситуацію, необхідно з'ясувати: чи не мав місце цивільно-правовий делікт; чи не мало місце адміністративне правопорушення; чи не помиляється потерпілий з приводу вчинених щодо нього дій; чи не навмисно потерпілий надає неправдиву інформацію про злочин, якого насправді не було; коли, де і як злочинці вчиняли дії з підготовки до вчинення злочину і які саме дії вчинялися ними; який вплив злочинці здійснювали у відношенні потерпілого (психологічний, фізичний тощо), де і коли здійснювалися злочинні дії щодо потерпілого; які були умови угоди і, якщо складався договір, то ким саме; які документи використовувалися у ході вчинення злочину; чи не має місце факт здійснення ряду злочинів під прикриттям тощо [23; 22].

Втім, як показало опитування респондентів, 95 % з них вважає дуже коротким термін 24 години, протягом яких слідчий повинен встановити підстави для відкриття кримінального провадження щодо шахрайства, пов'язаного з інтернет-комерцією. У такі стислі строки дуже складно

прийняти об’єктивне рішення, адже така категорія кримінальних правопорушень дуже часто знаходиться на межі з цивільно-правовими відносинами і, без проведення ряду заходів, дуже складно на початку визначити склад шахрайства. Без встановлення умислу ймовірним може бути у подальшому закриття кримінального провадження у зв’язку із відсутністю складу злочину через наявність цивільно-правових відносин, або встановлення неможливості виконати цивільно-правові зобов’язання у зв’язку із форсмажорними обставинами тощо.

Вивчаючи дану проблематику, Н. В. Глинська, Л. М. Лобойко та О. І. Марочкін наголошують на тому, що завданням службової особи правоохоронного органу, яка отримує джерело первинної інформації про ймовірно вчинене протиправне діяння (принаймні, якщо так вважає заявник), є визначення його попередньої правової кваліфікації. Звичайно, вона може зазнавати трансформації у перебігу юридичного процесу, що може мати наслідком зміну різновиду процесу (наприклад, із кримінального на адміністративний). Але на момент отримання і вивчення первинних відомостей, попри їх можливу обмеженість, правова кваліфікація діяння має бути встановлена обов’язково [34, с. 134].

Втім, опитування практичних працівників засвідчило, що під час оцінки первісної інформації про вчинений злочин при купівлі-продажу через мережу Інтернет, найбільші ускладнення виникають саме під час визначення попередньої правової кваліфікації кримінального правопорушення з зазначенням статті (частини статті) закону України про кримінальну відповідальність, відомості про які обов’язково необхідно зазначати під час внесення відомостей до ЄРДР згідно з п. 5 ч. 5 ст. 214 КПК. Правильна попередня правова кваліфікація кримінального правопорушення впливає на порядок проведення досудового розслідування (досудове слідство або дізнання) а також на вибір процесуальних заходів, які слідчий буде в подальшому здійснювати в межах розслідування кримінального правопорушення (наприклад – проведення негласних слідчих (розшукових)

дій). Проблема в тому, що злочинні дії з розміщення на певних сайтах неправдивої інформації про продаж неіснуючих товарів та отримання винним за них передоплати деякі суди кваліфікують як шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України). Інші суди подібні діяння перекваліфіковують на ч. 1 або ч. 2 ст. 190 КК України, обґрунтовуючи це тим, що перерахування грошей потерпілими на рахунок винного не є незаконною операцією з використанням електронно-обчислювальної техніки [176, с. 481; 205].

У таких випадках суди та правоохоронні органи залишають поза своєю оцінкою сам механізм злочинної дії – реєстрацію на сайтах, розміщення неправдивих оголошень, незаконне отримання передоплати тощо. Адже шахрайство, яке вчиняється за допомогою новітніх технологій, характеризується різноманітністю форм і способів, а ч. 3 ст. 190 КК України в чинній редакції не відображає всіх можливих способів учинення шахрайства, де принаймні використовуються засоби електронно-обчислювальної техніки, мережа Інтернет, мобільна телефонія тощо та пропонує замість терміну «електронно-обчислювальна техніка», що на її думку є застарілим, запровадити терміни «комп'ютерна система» й «телекомунікаційна мережа» [176, с. 487; 205].

У розрізі цього ряд вчених призиває до повернення інституту «дослідчої» перевірки [29, с. 237; 102].Натомість, є науковці, які категорично проти повернення інституту «дослідчої перевірки» [178].

Втім, хотілось би звернути увагу, що діяльність правоохоронних органів щодо реагування на події, які можуть містити в собі ознаки кримінального правопорушення, розпочинається трохи раніше. Адже «Порядком ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події», затвердженимнаказом МВС України від 08.02.2019 № 100, визначений чіткий алгоритм з прийняття та реєстрації в заяв і повідомлень про кримінальні правопорушення та інші події уповноваженими службовими особами органів

(підрозділів) поліції. За рішенням керівника органу (підрозділу) поліції або особи, яка виконує його обов'язки, відомості про виявлене кримінальне правопорушення уповноважена службова особа реєструє в ІТС ІПНП (журналі ЄО в разі тимчасової відсутності технічних можливостей унесення таких відомостей до ІТС ІПНП) та невідкладно, але не пізніше 24 годин реєстрації передаються до органу досудового розслідування для внесення відповідних відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР) [138].Тому, це і є своєрідним фільтром у відсіюванні фактів, які явно не мають ознак кримінального правопорушення.

І. А. Антонюк правильно зауважує, що проблема в тому, що витік часу для органів досудового розслідування розпочинається не з моменту надходження до них матеріалів, а з моменту подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення. Тобто, несвоєчасне надходження до слідчого (прокурора) матеріалів значно скорочує час для їх оцінки та прийняття об'єктивного рішення [5].

Разом з тим, можна зрозуміти, що невизначеність питання стосовно віднесення діяння до конкретного виду правових відносин, не дає підстави ігнорувати подію. У слідчого для прийняття рішення є 24 години, протягом яких він зобов'язаний з'ясувати, чи полягає суть певних правовідносин в площині цивільного права, чи виникли кримінально-правові відносини. Якщо є хоча б вірогідні дані вважати подію злочином, інформація вноситься до ЄРДР [198].

У цьому розрізі слід погодитися із Т. О. Мудряк, що невміння виділити ключові моменти початкової інформації, криміналістичні ознаки кримінального правопорушення, взаємозв'язки між окремими фактами, визначити характер і обсяг недостатніх відомостей, які необхідно отримати або уточнити, призводить до того, що слідчі, особливо на початковому етапі розслідування, проводять слідчі (розшукові) дії безсистемно,

нецілеспрямовано, а тому допускають безліч помилок, випускають з уваги найважливіші джерела доказової інформації, час і можливості їх вилучення й дослідження [112, с. 280].

Опитування практичних працівників та аналіз матеріалів кримінальних проваджень свідчить про те, що найчастіше первісна інформація про вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет, найчастіше отримується з наступних джерел:

- усна або письмова заява або повідомлення про вчинений злочин (усна заява або повідомлення вноситься до протоколу прийняття заяви про кримінальне правопорушення та іншу подію, а письмова заява або повідомлення приймається та реєструється);

- рапорт поліцейського про самостійне виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинений злочин [204; 205; 54].

Інформація про вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет отримується вкрай рідко з такого виду джерела як повідомлення осіб, що затримали підозрювану особу під час учинення або замаху на вчинення кримінального правопорушення чи безпосередньо після вчинення кримінального правопорушення, чи під час безперервного переслідування особи, яка підозрюється в його вчиненні. Причинами такого стану речей є технічна сторона способу вчинення злочину; географічне розташуванням зловмисника та потерпілого; велика розбіжність у часі між вчиненими діями та настанням наслідків [158, с. 27-28; 204].

Водночас, О. А. Самойленко розширює типові джерела оперативної інформації про кіберзлочини, серед яких називає:

- електронні та письмові повідомлення про злочин;

- запити і повідомлення правоохоронних органів інших держав, міжнародних правоохоронних організацій (в результаті перевірки цієї інформації співробітниками ДКП складається рапорт (ст.6 Закону України «Про оперативно-розшукову діяльність»);

- матеріали, складені в результаті перевірки заяв і повідомлень громадян, з якими встановлено негласне співробітництво (в результаті перевірки цієї інформації співробітниками ДКП складається рапорт (ст.6 Закону України «Про оперативно-розшукову діяльність»);

- матеріали інших правоохоронних органів;

- інші відомості, отримані унаслідок оперативно-розшукової діяльності (в результаті оперативного пошуку). Слідчі НП України, СБ України під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні також можуть виявити кіберзлочин [154, с. 22].

У зв'язку із цим О. В. Курман акцентує, що, крім матеріалів, одержаних процесуальним шляхом при плануванні розслідування, вивчається також інформація, зібрана оперативним шляхом [97, с. 88].Натомість, для того щоб оперативна інформація про вчинення злочину була перспективною з позицій відкриття кримінального провадження, вона має бути підтверджена достовірними для слідчого джерелами, які закономірно пов'язані з документальністю факту її перевірки оперативним підрозділом, що оформлюється у вигляді матеріалів первинної перевірки. Ці матеріали підлягають передачі керівнику органу досудового розслідування з метою внесення викладеної інформації до ЄРДР. Водночас варто акцентувати на оцінній діяльності начальника слідчого відділу/ слідчого щодо матеріалів такої перевірки інформації про злочин. За умови неповноти та недостовірності інформації отримані слідчим матеріали перевірки повертають до оперативного підрозділу для доопрацювання з рекомендаціями щодо подальших дій суб'єкта перевірки. Тому для вирішення питання про відкриття кримінального провадження для слідчого особливого значення набувають офіційні документи, що підтверджують оперативну інформацію, та розуміння ним компетенції суб'єктів первинної перевірки, власне такі компетенції зумовлюють особливості здійснення останньої [155, с. 167].

Оскільки на початковому етапі розслідування основним і значущим фактором є час, то дії слідчого та оперативних співробітників на цьому етапі повинні характеризуватися максимальною мобільністю. На цьому наголошує й Є. П. Бєгалов, тому, що значна кількість злочинів розкривається саме завдяки оперативному реагуванню на протиправну подію. Раптовість виступає в таких випадках найважливішим засобом подолання протидії, тому, ефективність розслідування вищезазначених злочинів значно підвищується при внесенні відомостей про кримінальне правопорушення до ЄРДР за матеріалами, зібраними в процесі здійснення оперативно-розшукових заходів. У таких випадках часто складається ситуація, при якій слідчий і оперативний співробітник заздалегідь можуть вивчити наявну інформацію і визначити час, порядок і послідовність її використання з метою досягнення бажаного результату. Їх дії, таким чином, приймають цілеспрямований, плановий характер, в той час, коли заінтересовані у протидії розслідуванню особи їх не очікують. Це дозволяє навіть своєчасно здійснити затримання всіх підозрюваних та їх співучасників і виключити можливість узгодження ними своїх дій [13, с. 97].

Як показав аналіз кримінальних проваджень, опитування респондентів, на початку кримінального провадження слідчий активно співпрацює з працівниками Департаменту кіберполіції України, до яких насамперед надходять заяви та повідомлення про вчинення шахрайства, пов’язаного із електронною комерцією, які активно взаємодіють із іншими органами Національної поліції та виступають помічниками у розкритті таких кримінальних правопорушень.

Завданнями Департаменту кіберполіції є «сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам НП України у попередженні, виявленні та припиненні кримінальних правопорушень». Отже, для низки підрозділів у складі НП України основним джерелом інформації про злочин, вчинений у кіберпросторі, часто є матеріали Департаменту кіберполіції НП України [155, с. 149].

Наведемо приклад. Так, за оперативною інформацією співробітників відділу протидії кіберзлочинам у Миколаївській області було відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство) КК України. Двоє мешканців смт. Братське у соцмережах створювали так звані інтернет-магазини. Зловмисники орієнтувалися під запити населення і пропонували товари, що мають попит, зокрема військовий тактичний одяг та генератори. Для просування інтернет-сторінок використовували рекламу. Умовою купівлі була повна передоплата на банківські картки. Однак, отримавши гроші, чоловіки не виконували взятих на себе зобов'язань. Клієнтам повідомляли, що нібито потрібно ще зачекати, бо товари доставляють з-за кордону. Надалі зловмисники блокували покупців [124].

Також, до ГСУ НП України 11.04.2019 надійшов рапорт працівників Департаменту оперативної підтримки НП України про те, що на офіційному сайті ОСОБА_1 і команди за відповідним інтернет посиланням виявлено публікацію, яка містить незаконні дії. Крім цього, відповідно до наданих матеріалів встановлено, що вказаний відеоматеріал був розміщений на каналах у соціальних мережах Viber - euua.org/v та Telegram - euua.org/t. Посилання на вказані канали у соціальних мережах можливо отримати після реєстрації на сайті euua.org. В ході проведення досудового розслідування працівникам Департаменту кіберполіції НП України було надано доручення в порядку ст. 40 КПК України, направленого на встановлення першоджерела розповсюдження вищевказаного відеозапису. У відповідь на вказане доручення надійшов мотивований рапорт про те, що було проведено огляд веб-ресурсу euua.org/t та встановлено ймовірну особу, яка може бути причетною до вчинення вказаного кримінального правопорушення, а саме ОСОБА_2, ІНФОРМАЦІЯ_1. Крім цього, під час аналізу наявної інформації оперативним шляхом було встановлено IP-адресу, з якої користувач соціальної мережі «Facebook» ОСОБА_3 розмістив на своїй сторінці відеозапис під назвою «ІНФОРМАЦІЯ_3», а саме: ІНФОРМАЦІЯ_2. Вказана IP-адреса у проміжок часу розміщення відеозапису Інтернет провайдером

ТОВ «Воля кабель» надавалась у користування абоненту за адресою: АДРЕСА_1. В ході проведення огляду сторінки інтернет сайту від 20.05.2019 встановлено наявність на авторизованій особистій сторінці користувача ОСОБА_2 у мережі «Facebook» відеозапису під назвою «ІНФОРМАЦІЯ_3», який був розміщений 10 квітня 2019 року. Крім цього, в ході проведення огляду telegram-каналу «Європейське майбутнє України» від 20.05.2019 встановлено наявність розміщеного аналогічного відеозапису, який було розміщено 10.04.2019 о 21 год. 34 хв. На момент проведення огляду встановлено, що відеозапис перебуває у відкритому доступі. 11.05.2019 на адресу Інтернет провайдера ТОВ «ВОЛЯ-КАБЕЛЬ» направлено запит з метою встановлення обставин надання доступу до мережі Інтернет абоненту за адресою: АДРЕСА_1. 24.06.2019 у відповідь на запит від ТОВ «Воля-Кабель» надійшла відповідь про неможливість надання запитуваної інформації із посиланням на п. 7 ч. 1 ст. 162 КПК України, відповідно до якої інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв`язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо – відноситься до речей та документів, які містять охоронювану законом таємницю, а відтак у сторони обвинувачення звернулася щ даним клопотанням. Внаслідок чого слідчий суддя надав дозвіл на тимчасовий доступ на такі об’єкти [165].

Згідно Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, затвердженої наказом МВС України № 575 від 07.07.2017 р., матеріали оперативного підрозділу, у тому числі Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп’ютерів, систем та комп’ютерних мереж і

мереж електрозв'язку, направляються до слідчого підрозділу для початку та здійснення досудового розслідування із відповідними зібраними матеріалами. При цьому, матеріали оперативного підрозділу, у тому числі Департаменту кіберполіції Національної поліції України, його структурного підрозділу, який діє за міжрегіональним принципом, де зафіксовано фактичні дані про кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, що направляються до слідчого підрозділу для початку та здійснення досудового розслідування, мають містити:

- письмове пояснення заявника, в якому зафіксовані відомі заявнику дані про вчинення кримінального правопорушення з відповідними додатками, що містять відомості, які підтверджують його вчинення (роздруківки або скріншоти (програмне фотографування зображення з екрана монітора) вікон програм), а також у разі наявності документи, що підтверджують право власності потерпілого на комп'ютерну інформацію та інформацію, що передається мережами електрозв'язку, чи програмно-технічні засоби;

- установлені ідентифікаційні дані про використані електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку (логін і пароль для доступу до мережі Інтернет, IP-адреса, WEB-адреса, номер абонента мережі електрозв'язку чи номер телефону, за допомогою яких було здійснено такий доступ, тощо) [143].

Також, джерелом інформації про шахрайство, пов'язане з електронною комерцією, може бути інформація, отримана від служби безпеки Банку про незаконні транзакції. Звісно, реалізація такої інформації здійснюватиметься тільки у взаємодії з Департаментом кіберполіції та органами Національної поліції України.

У такий спосіб було викрито протиправну діяльність ОЗГ, члени якої знаходили оголошення щодо продажу товарів на тематичних платформах та

для обговорення деталей писали продавцям у сторонні месенджери. Туди зловмисники надсилали фішингові посилання нібито про інтернет-оплату. Коли продавці переходили за посиланням та вводили дані банківської карти, ці відомості одразу ставали відомі шахраям. Отримавши доступ до банківських рахунків, зловмисники переводили гроші потерпілих на підконтрольні картки, оформлені на третіх осіб. Встановлено, що у такий спосіб вони привласнили понад 400 тисяч гривень [184].

Слід сказати, що, згідно Закону України «Про електронну комерцію» електронний договір вважається укладеним з моменту одержання особою, яка направила пропозицію укласти такий договір, відповіді про прийняття цієї пропозиції в порядку, визначеному частиною шостою цієї статті. При цьому, місцем укладення електронного договору є місцезнаходження юридичної особи або місце фактичного проживання фізичної особи, яка є продавцем (виконавцем, постачальником) товарів, робіт, послуг. Момент виконання продавцем обов’язку передати покупцеві товар визначається згідно з положеннями Цивільного кодексу України про купівлю-продаж, якщо інше не встановлено цим Законом [142; 205].Проте, як показав аналіз судово-слідчої практики та опитування практичних працівників, які розслідували кримінальні правопорушення, пов’язані із вчиненням шахрайських дій через мережу Інтернет, на початку кримінального провадження найбільші складнощі виникають саме при встановлення територіальної юрисдикції, в межах якої вчинено кримінальне правопорушення. Це стає причиною неодноразової передачі матеріалів кримінального провадження за територіальною підслідністю із одного району підрозділу Національної поліції до іншого. Часто матеріали передаються за межі регіону, в якому розпочате кримінальне провадження [54].

С. В. Чучко пояснює цей факт тим, що у разі чіткого визначення місця вчинення кримінального правопорушення проблем немає і досудове розслідування здійснюється слідчим того органу досудового розслідування, під юрисдикцією якого знаходиться це місце. Разом з тим, у разі якщо місце

вчинення кримінального правопорушення невідоме або його вчинено за межами України, місце проведення досудового розслідування визначає відповідний прокурор. Згідно п. 3 ст. 218 КПК України, таке місце визначається з урахуванням місця виявлення ознак кримінального правопорушення, місця перебування підозрюваного чи більшості свідків, місця закінчення кримінального правопорушення або настання його наслідків тощо. Тобто, вбачається альтернативний варіант, який залежить від ряду обставин та тлумачення цієї норми прокурором [205].

Отже, основним завданням перевірки заяв і повідомлень про шахрайство в інтернет-комерції, а також оцінки матеріалів самостійного виявлення посадовою особою правоохоронних і контролюючих державних органів щодо фактів вчинення чи підготовки до таких кримінальних правопорушень, є з'ясування наявності достатніх приводів та підстав для відкриття провадження. Не менш важливим завданням є також встановлення попередньої правової кваліфікації, а також вибір процесуальних заходів, найбільш доцільних для прийняття об'єктивного рішення.

2.2. Організація та планування розслідування шахрайства в інтернет-комерції, та коло обставин, що підлягають встановленню

Ефективність та якість вирішення тактичних завдань залежить від правильної організації процесу розслідування, що включає комплекс необхідних заходів, які забезпечують діяльність органів досудового розслідування з виявлення, розслідування та попередження кримінальних правопорушень на різних етапах розслідування.

До організаційних дій із розслідування конкретного кримінального правопорушення слід віднести залучення необхідних сил і засобів, налагодження взаємодії з оперативними підрозділами та іншими

правоохоронними органами, мобілізація учасників розслідування, керівництво та координація дій учасників розслідування, а також планування розслідування [121, с. 80].Втім, слід зауважити на різноманітності поглядів з приводу співвідношення понять «організація розслідування» та «планування розслідування».

Ми схиляємося до думки, що поняття «організація розслідування» та «планування розслідування» невід'ємні одне від одного. Так, планування виражається у вигляді запланованих заходів (у тому числі висуненні версій, визначенні обставин, які підлягають встановленню, з'ясуванні слідчої ситуації, що склалася на певному етапі розслідування), застосуванні певних техніко-криміналістичних та інших наукових засобів, визначенні строків і виконавців. Організація хоча і є ширшим поняттям, але завдяки їй здійснюється реалізація наміченого плану, його адаптація та динамічність відповідно до новостворених обставин. Зокрема, організація передбачає: 1) створення найбільш оптимальних умов для виконання запланованих заходів (проведення слідчих (розшукових), негласних слідчих (розшукових), оперативно-розшукових заходів тощо), враховуючи як процесуальні, так і тактичні аспекти; 2) застосування найбільш ефективних шляхів і способів реалізації поставлених завдань розслідування; 3) забезпечення узгодженості та упорядкованості дій органів і осіб при вирішенні цих завдань. Правильно організоване планування дає можливість проводити розслідування цілеспрямовано, дозволяє закінчити слідство в установлені законом строки, дисциплінує слідчого, забезпечує повноту та об'єктивність слідства, сприяє одержанню максимуму ефекту при найменшій затраті слідчим часу, сил і коштів [126].

Велике значення має й визначення криміналістичних особливостей початкового етапу розслідування шахрайства у кіберпросторі, його значення, аналіз та обґрунтування як одного з видів кіберзлочинності, що є небезпечним для кожного [229, с. 141].

Виходячи з цього, можна сказати, що організація розслідування отримує матеріалізацію у плані розслідування [152, с. 200; 90].При цьому, планувати розслідування необхідно таким чином, щоб було прийнято всі передбачені законом заходи для забезпечення своєчасного, всебічного, повного та об'єктивного розслідування злочину і підвищення рівня організації для досягнення ефективного кінцевого результату [107, с. 36; 126].

Як показав аналіз вивчення матеріалів кримінальних проваджень, у планах розслідування шахрайства в інтернет-комерції в основному відображалися такі елементи планування розслідування: 1) побудова слідчих версій (73 %); 2) визначення обставин, що підлягають установленню (98 %); 3) визначення заходів, за допомогою яких слід вирішувати завдання розслідування (СРД, НСРД, ОРЗ, організаційні заходи (100 %); 4) визначення строків вирішення окремих завдань (100 %); 5) визначення виконавців та виконавців контролю (100 %); 6) налагодження взаємодії слідчого зі співробітниками оперативних підрозділів, іншими органами та спеціалістами (95 %); 7) визначення науково-технічних засобів, спрямованих на виконання завдань розслідування (38%) тощо.

Натомість, процес планування є динамічним і план може постійно доповнюватися додатковими позиціями, залежно від обставин справи та отримання нових доказів.

Виходячи з цього, можна побачити, що в основі планування будь якого розслідування на його початку відбувається висунення загальних та приватних версій.

Версія – це обґрунтоване припущення, що стосується сутності розслідуваного кримінального правопорушення або його окремих обставин, що має значення для його розслідування і пояснює походження, зміст і зв'язок між цими обставинами [89, с. 311].

Як показали результати опитування уповноважених осіб, які розслідували шахрайства в інтернет-комерції, та аналіз матеріалів

кримінальних проваджень, в даній категорії кримінальних проваджень висувалися такі загальні версії:

- шахрайство в інтернет-комерції мало місце за обставин, які повідомив потерпілий;

- шахрайство в інтернет-комерції мало місце, але за інших обставин;

- вчинено інше кримінальне правопорушення;

- ознаки шахрайства відсутні, заявник помиляється стосовно події, що відбулась.

Одночасно необхідно висувати версії стосовно осіб, які можуть володіти необхідною інформацією про шахрайство (свідків), зокрема:

- інформацією про шахрайство володіють інтернет-провайдери;

- інформацією про шахрайство володіють банківські працівники;

- інформацією про шахрайство володіють працівники поштових відділень;

- інформацією про шахрайство володіють працівники приватного підприємства та фізичні особи, які укладали дистанційні правочини;

- інформацією про шахрайство володіють особи з кола знайомих запідозреної службової особи тощо.

До приватних версій можна віднести:

- шахрайство вчинено організованою групою, яка спеціалізується на кібершахрайствах;

- шахрайство вчинено організованою групою, яка спеціалізується на кібершахрайствах та інших злочинах;

- шахрайство вчинено за попередньою змовою групою осіб;

- шахрайство вчинено особами, раніше судимими за аналогічні кримінальні правопорушення;

- шахрайство вчинене раніше не судимими особами.

Загалом, успіх розслідування залежать від здобутих вже на початковому етапі фактичних даних, що підтверджують як факт вчинення кримінального правопорушення, так і причетність певних осіб до його вчинення. А звідси

завдання, які слідчий, залежно від обставин, що склалися вже визначає на початковому етапі розслідування безпосередньо залежать від змісту отриманих відомостей на момент їх внесення до ЄРДР [63].

Необхідною практичною діяльністю планування є визначення обставин, що підлягають установленню в процесі розслідування кримінальних правопорушень [45, с. 114].

Слід зазначити, що у ст. 91 КПК України надається вичерпний перелік обставин, які підлягають доказуванню у кримінальному провадженні:

1) подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

3) вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат;

4) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом’якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження;

5) обставини, що є підставою для звільнення від кримінальної відповідальності або покарання;

6) обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов’язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані

або використані як засоби чи знаряддя вчинення кримінального правопорушення;

7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру [94].

Натомість, ми схиляємося до думки, що перелік обставин, які підлягають встановленню, є набагато ширшим, ніж обставини, що підлягають доказуванню, і залежить від конкретних тактичних завдань, які необхідно вирішити на певному етапі, виходячи з типової слідчої ситуації, що склалася. Разом з тим, всі ці обставини витікають з предмета доказування і не виходять за його межі. Межі доказування – це такий обсяг доказового матеріалу (доказів та їх джерел), який забезпечить надійне, достовірне встановлення всіх обставин, що входять до предмета доказування, правильне вирішення справи та вжиття заходів для запобігання злочинам. Хоча необґрунтоване розширення меж доказування і зумовлює отримання таких доказів, які вже достовірно встановлені або взагалі можуть не стосуватися відповідного кримінального провадження, що, у свою чергу, призводить до затягування досудового розслідування та судового розгляду, що негативно впливає на самих учасників кримінального провадження. В свою чергу, звуження меж доказування призводить до того, що окремі обставини кримінального провадження недостатньо або не в повній мірі досліджуються і, як наслідок, у кримінальному провадженні з’являються прогалини у встановленні тих чи інших обставин злочину, що не дозволяє, всебічно, повно і неупереджено розслідувати кримінальне провадження, розглядати його під час судового розгляду та приймати відповідне законне та обґрунтоване процесуальне рішення [167; 109, с. 106; 198].

У цьому розрізі А. В. Журавель вважає, що під час досудового розслідування вирішується широке коло завдань, основними з яких є стратегічні, що випливають з предмета доказування, та локальні, які мають ситуаційну зумовленість та підлягають встановленню під час розслідування окремого різновиду кримінальних правопорушень [60, с. 201].

При розслідуванні конкретного кримінального провадження виникає необхідність дослідження суттєвих обставин, обумовлених притаманними тільки цьому провадженню. В силу цих же причин окремі обставини і питання, які підлягають дослідженню, можуть відпасти, характер їх може змінитися. Знання важливих обставин, які підлягають вставленню дає можливість слідчому уникати непотрібних дій, обирати правильний, найбільш раціональний шлях дослідження, підвищувати тим самим ефективність слідства, економити час [108, с. 144].

Говорячи про обставини, що підлягають встановленню при розслідуванні шахрайства в інтернет-комерції, слід враховувати, що особистий контакт між потерпілим і шахраєм в основному здійснюється дистанційно, так само і спосіб переправлення грошей, що ускладнює суттєво розслідування та процес встановлення злочинця.

До того ж, обстановка вчинення Інтернет шахрайства характеризується найчастіше відсутністю свідків [151, с. 53], а обман при вчиненні шахрайства може виразитися у застосуванні програмних засобів, які дають змогу винному будь-яким чином (шляхом відшукування випадкових цифр, паролів тощо) здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в автоматизованих системах, щоб ввести в оману автоматизовану систему і видати себе за того, хто має право в ній працювати і здійснювати відповідні операції. Проникнувши у такий спосіб до відповідної електронної системи, шахрай може вплинути на процес обробки інформації, перекрутити її зміст чи знищити, налагодити систему так, щоб вона функціонувала в режимі, який би сприяв вчиненню незаконних дій. Суть обману в тому, що він реалізується за допомогою використання електронно-обчислювальної техніки, що потребує наявності відповідних знань, рівня підготовки, навичок [117 с. 480].

В контексті даної проблематики С. В. Чучко запропонував поділити на певні групи обставини, що підлягають встановленню, під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет, зокрема:

1) обставини, що стосуються події шахрайства при купівлі-продажу товарів через мережу Інтернет (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його вартості; розміщення фейкової інформації про продаж товару за умов накладного платежу з подальшим отриманням частини його вартості на платіжну карту (передоплати); створення сайтів магазинів у мережі Інтернет або їх копій, що діють за принципом фірм-одноденок; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати тощо); відомості про знаряддя (засоби) злочину; відомості про сліди злочину; відомості про предмет злочинного посягання (його кількісні та якісні характеристики), тощо);

2) обставини, що стосуються особи потерпілого та злочинця (ознаки суб'єкта злочину: фізична особа, осудність, вік, кваліфікуючі ознаки, які стосуються суб'єкта; кількість злочинців (наявність розподілу ролей серед шахраїв, функції кожного з них);

3) причинкові обставини: наявність причинного зв'язку між діями винних осіб та їх наслідками; виявлення причин та умов, які сприяли вчиненню злочину; заходи, яких необхідно вжити для їх усунення тощо;

4) решта обставин (вид і розмір шкоди, завданої кримінальним правопорушенням; кваліфікуючі ознаки щодо розміру шкоди завданої злочином; обставини, що обтяжують чи пом'якшують покарання; обставини, що виключають кримінальну відповідальність, чи є підстава для закриття кримінального провадження; обставини, що є підставою для звільнення від кримінальної відповідальності, а також обставини, що виключають факт вчинення підозрюваною особою іншого злочину тощо [205; 206].

Схожий розподіл обставин, що підлягають встановленню, й у Т. В. Коршикової. Так, вчена у кримінальному провадженні щодо шахрайства, учиненого з використанням ЕОТ, всі обставини, що підлягають встановленню, вважає доцільним об'єднати у наступні групи:

1) обставини, що стосуються самої події кримінального правопорушення. До цієї категорії потрібно зараховувати відомості про подію кримінального правопорушення, зокрема: 1) чи був факт вчинення шахрайства; 2) було вчинене шахрайство чи мало місце інсценування кримінального правопорушення; 3) чи використовувалось під час шахрайства ЕОТ; 4) час і місце вчинення шахрайства; 5) способи вчинення шахрайства та які дії здійснював злочинець для підготовки та приховування кримінального правопорушення; 6) які сайти, вебпортал чи соціальні мережі використовувалися для вчинення шахрайства; 7) яким чином були переведені (надані) кошти злочинцю; 8) хто був очевидцем вчинення шахрайства;

2) винуватість підозрюваного у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

3) вид і розмір шкоди, завданої кримінальним правопорушенням, а саме відомості про предмет злочинного посягання (його кількісні та якісні характеристики), яким виступатиме майно, яке було ввірене винному чи було в його віданні, тобто воно знаходилось у правомірному володінні винного, який був наділений правомочністю з розпорядження, управління, доставки або зберігання такого майна. До того ж, відповідно до п. 3 ч. 1 ст. 91 КПК України у кримінальному провадженні підлягає доказуванню також розмір процесуальних витрат [81, с. 100-101].

4) відомості, що характеризують особу підозрюваного. До таких відомостей належать дані про: вік особи, стан її здоров’я, поведінку, взаємини, колишні судимості тощо. До суб’єктивних чинників потрібно віднести: наявність у злочинців попереднього злочинного досвіду, зокрема й знання ЕОТ, сфери комунікаційного зв’язку, конкретних способів учинення, приховування слідів у мережі Інтернет, індивідуальні властивості особи злочинця тощо;

5) обставини, які пом’якшують або обтяжують покарання, що відображено в ст. ст. 66 і 67 КК України;

6) обставини, які звільнюють від кримінальної відповідальності. Для правильного трактування сутності обставин, за наявності яких законодавець або взагалі виключає злочинність і караність діяння (тим самим особу не притягують), або вважає недоцільним притягнення особи до кримінальної відповідальності (тобто особа звільняється від кримінальної відповідальності), найважливіше значення має розгляд ознак кримінального правопорушення, які й визначають його поняття;

7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру. Перелік таких підстав міститься в КК України. Так, зокрема, в ст. 963 КК України визначено, що однією з підстав для застосування до юридичної особи заходів кримінально-правового характеру є вчинення її вповноваженою особою від імені юридичної особи будь-якого кримінального правопорушення [81, с. 103].

Проаналізувавши підходи різних учених та здійснивши аналіз кримінальних проваджень щодо шахрайства в інтернет-комерції, виділимо наступні типові обставини, що підлягають встановленню:джерело надходження інформації про подію шахрайства в інтернет-комерції;наявність факту кримінального правопорушення (чи дійсно дії, пов’язані із торгівлею в мережі Інтернет, є злочинними, чи мав місце цивільно-правовий делікт);в чому полягали підготовчі дії, дії з безпосереднього вчинення та приховування шахрайства, яка їх тривалість, де вони відбувалися; кількість епізодів злочинної діяльності;час та місце вчинення шахрайських дій;обставини, які характеризують особу потерпілого;обставини, які характеризують особу шахраїв, їх кількість та характер участі кожного у вчиненні шахрайства в інтернет-комерції; обставини, доводять ознаки організованого злочинного угруповання;обставини, що підтверджують вину кожного з шахраїв;обставини, що виключають кримінальну відповідальність;обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, обтяжують чи пом’якшують покарання кожного співучасника;обставини, що підтверджують вид і розмір завданої

шкоди;наявність злочинних зв’язків шахраїв із представниками влади та особами, які супроводжують дистанційні правочини щодо купівлі-продажу товарів та послуг через мережу Інтернет.

Серед приватних обставин можна назвати наступні:приналежність та 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 яких здійснювався доступ, необхідний для укладання угоди через мережу Інтернет тощо.

З цього приводу Е. Ансельмо зазначає, що кожний користувач мережі Інтернет і його комп’ютер діють автономно та формують єдину транснаціональну мережу, яка виходить за межі географічної концепції чітких кордонів. Поряд із погодженням твердження про нематеріальний (віртуальний) характер інтернет-адреси, а також адрес сайтів, що містять URL-індикатори країни походження, вчений акцентує увагу, що сервери переміщаються у фізичному просторі [3, с. 27]. Виходячи з цього, актуальним питанням є встановлення точок доступу, з яких здійснювалося спілкування між покупцем та продавцем.

Для ідентифікації особи правопорушника необхідно встановити: коло осіб, які користуються певним терміналом, а також мету та межі їх користування; технічну підготовку та навички користування певними програмними та технічними засобами; осіб, які користувалися терміналом під час вчинення протиправних дій; хто має доступ до мережі Інтернет, які при цьому використовуються логіни та паролі, через якого провайдера; з яких ще IP-адрес використовувались дані реквізити при доступі до мережі тощо. Отримання інформації у відкритих джерелах мережі Інтернет. До відкритих джерел відносяться: соціальні мережі, телефонні довідники, мобільні

додатки, державні реєстри, сервіси які потребують реєстрації та на яких потрібно вказувати достовірні персональні дані [154, с. 24].

Для встановлення права продавця на здійснення дистанційного правочину, відповідно, встановлення його на причетність шахрайству – слід з’ясувати офіційні правила здійснення інтернет-торгівлі. Так, продавцями у сфері електронної комерції можуть бути суб'єкти господарської діяльності (юридичні та фізичні особи). Таку діяльність здійснюють відповідно до класу 47.91 «Роздрібна торгівля, що здійснюється фірмами поштового замовлення або через мережу Інтернет» національного класифікатора ДК 009:2010 «Класифікація видів економічної діяльності», затвердженого наказом Державного комітету з питань технічного регулювання та споживчої політики від 11.10.2010 р. № 457. У Методосновах № 396 указано, що клас 47.91 охоплює роздрібну торгівлю з допомогою компаній поштового замовлення або мережі Інтернет, тобто діяльність із роздрібної торгівлі, де покупець робить свій вибір, ґрунтуючись на рекламних оголошеннях, каталогах, інформації вебсайтів чи будь-якій іншій рекламній продукції, та здійснює замовлення поштою, телефоном або через мережу Інтернет (зазвичай за допомогою спеціальних засобів, розміщених на вебсайті). Товар, що купується, може бути або безпосередньо завантажений з інтернет-сайта, або доставлений покупцеві. Цей клас охоплює: роздрібну торгівлю будь-якими товарами з допомогою компаній поштового замовлення; роздрібну торгівлю будь-якими товарами в мережі Інтернет; а також пряму торгівлю за допомогою телебачення, радіо та за телефоном; діяльність із роздрібної торгівлі інтернет-аукціонів [26]. Відповідно до ч. 1 ст. 7 Закону № 675 продавець (виконавець, постачальник) товарів, робіт, послуг в електронній комерції під час своєї діяльності та в разі поширення комерційного електронного повідомлення зобов'язаний забезпечити іншим учасникам відносин у сфері електронної комерції прямий, простий, стабільний доступ до такої інформації: повне найменування юридичної особи або прізвище, ім'я, по батькові фізичної особи – підприємця;

місцезнаходження юридичної особи або місце реєстрації та місце фактичного проживання фізичної особи – підприємця; адреса електронної пошти та/або адреса інтернет-магазину; ідентифікаційний код – для юридичної особи, або реєстраційний номер облікової картки платника податків – для фізичної особи – підприємця, або серія та номер паспорта – для фізичної особи – підприємця, яка через свої релігійні переконання відмовилася від прийняття реєстраційного номера облікової картки платника податків, офіційно повідомила про це відповідний податковий орган і має відмітку в паспорті; – відомості про ліцензію (серія, номер, строк дії та дата видачі), якщо господарська діяльність підлягає ліцензуванню; щодо зарахування податків до розрахунку вартості товару, роботи, послуги, а в разі доставки товару – ще й інформація про вартість доставки; інші відомості, що відповідно до законодавства підлягають оприлюдненню [26].

Згідно Закону України «Про електронну комерцію», до таких «інших відомостей», зокрема, належить наступна інформація: 1) найменування продавця (виконавця), його місцезнаходження та порядок прийняття претензії; 2) основні характеристики продукції; 3) ціна, включно з платою за доставку, й умови оплати; 4) гарантійні зобов'язання та інші послуги, пов'язані з утриманням чи ремонтом продукції; 5) інші умови постачання або виконання договору; 6) мінімальна тривалість договору, якщо він передбачає періодичні постачання продукції або послуг; 7) вартість телекомунікаційних послуг, якщо вона відрізняється від граничного тарифу; 8) період прийняття пропозицій; 9) порядок розірвання договору. У разі ненадання вказаної інформації до суб'єкта господарювання можуть бути застосовані санкції, передбачені ст. ст. 15 та 23 Закону № 1023 [142].

В контексті даної проблематики, слід сказати, що 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 тощо).

Слід погодитися із О. В. Олішевським, який наголошує, що переважна більшість розслідувань пов'язана із взаємодією, оскільки слідчий сам не в змозі, або не вправі виконати певну дію [122, с. 231]. А. Я. Хитра формулює дану категорію як засновану на законі та спільності завдань у кримінальному судочинстві погоджену колективну діяльність, яка передбачає ефективне використання правових заходів і сил слідчих, обумовлена їх компетенцією та формами діяльності, спрямована на розслідування та попередження злочинів [193, с. 6].

Втім, А. В. Одерій та А. О. Шульга акцентують, що однією з важливих умов успіху в розкритті злочинів є правильна організація взаємодії відповідних органів, які беруть участь в цій діяльності, які, хоча і не підпорядковані, але діють узгоджено, ефективно застосовуючи методи та способи боротьби зі злочинами [119, с. 39]. В той же час, А. Я. Дубинський та Ю. І. Шостак також підтримують позицію щодо розгляду взаємодії правоохоронних органів як діяльності незалежних один від одного в адміністративному відношенні органів, що виражається в найбільш доцільному сполученні властивих цим органам засобів і методів, спрямована при організуючій ролі слідчого на попередження, припинення, розкриття та всебічне, повне й об'єктивне розслідування злочинів [47, с. 5].

У цьому розрізі можна вести мову про взаємодію із постачальниками електронних комунікаційних послуг, операторами послуг платіжної інфраструктури, адміністраторами, що присвоюють мережеві ідентифікатори, та іншими суб'єктами, що забезпечують передачу та зберігання інформації з використанням інформаційно-комунікаційних систем, а також банківськими представництвами.

З огляду на анонімність, можливість використання шахраями систем зв'язку з вільним доступом, придбання необмеженої кількості «sim-card»,

створення акаунтів на різних ресурсах, сервери яких розташовані і належать різним країнам, суттєво ускладнюють практичний бік боротьби із зазначеним видом шахрайств. Крім того, наявність низки бюрократичних складових під час виконання запитів щодо розслідування фактів Інтернет-шахрайства зводить нанівець роботу правоохоронців через великі терміни проходження документів. Компанії-власники серверів Інтернет-ресурсів не забезпечують зберігання всього обсягу даних, що проходить через їх устаткування довгий період часу. А тому від швидкості, своєчасності і сумлінності виконання запиту щодо злочину повною мірою залежить рівень ефективності розслідування. правоохоронці можуть результативно діяти лише використовуючи власні контакти у структурах, що зобов'язані виконувати зазначені запити, повідомляючи заздалегідь про вчинений злочин, а також запит, який надійде згодом, та отримують загальну інформацію щодо існування необхідних даних, місця знаходження злочинців, самого факту злочину [209, с. 63].

До того ж, серед уповноважених службових осіб правоохоронних органів, котрі взаємодіють зі слідчими підрозділами та прямо або опосередковано здійснюють виявлення кіберзлочинів та взаємодіють між собою, можна вказати наступні:

- підрозділи Департаменту кіберполіції, які згідно з п. 2.1. Положення про ДКП НП України, уповноважені щодо протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. ДКП є міжрегіональним територіальним органом, юридичною особою публічного права. До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту;

- інші оперативні підрозділи НП (Департамент карного розшуку, або Департаменту захисту економіки тощо), що здійснюють протидію іншим,

альтернативним Конвенції, злочинам, що вчиняються у кіберпросторі та підслідні слідчим НП України. ДКП стосовно таких злочинів можуть тільки сприяти в порядку, передбаченому чинним законодавством, іншим підрозділам НП України у попередженні, виявленні та припиненні кримінальних правопорушень – забезпечує своєчасне отримання інформації про злочини, що вчинені в кіберпросторі, або відповідні злочинні наміри;

- підрозділи контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, захисту національної державності Служби безпеки (ДКІБ СБ України). До завдань СБ України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України [154, с. 22].

В розрізі цього слід зауважити, що взаємодія відбувається не тільки між органами, які не підпорядковані один одному, а й між уповноваженими особами, які згідно кримінально-процесуального законодавства, повинні виконувати доручення органів досудового розслідування та їм підпорядковуватися за певних умов.

Підтвердженням є ч. 3 ст. 40 КПК України, згідно якої органи досудового розслідування мають право доручати проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій відповідним оперативним підрозділам[94], а також Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні. Так, згідно п. 8 цього нормативного акта слідчий (дізнавач) на місці події керує діями інших членів СОГ та відповідає за якість проведення огляду місця події; разом з іншими членами СОГ, залученими спеціалістами, запрошеними потерпілими, свідками та іншими учасниками кримінального провадження в установленому КПК України порядку [143].

Цією ж Інструкцією визначені особливості організації взаємодії при досудовому розслідуванні кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів). Зокрема, досудове розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку здійснюється слідчими, які спеціалізуються на розслідуванні кримінальних правопорушень зазначеного виду. При цьому, утворення СОГ за участю оперативних працівників Департаменту кіберполіції Національної поліції України, його структурних підрозділів, які діють за міжрегіональним принципом, для розслідування кримінальних правопорушень у сфері використання комп`ютерів, систем та комп`ютерних мереж і мереж електрозв`язку здійснюється за спільним наказом керівників органу досудового розслідування та Департаменту кіберполіції Національної поліції України. Утворення СОГ у кримінальному провадженні, досудове розслідування у якому здійснюється Головним слідчим управлінням Національної поліції України, здійснюється за наказом Голови Національної поліції України або за наказом заступника Голови Національної поліції України - начальника Головного слідчого управління, погодженим керівництвом Департаменту кіберполіції Національної поліції України. Старшим СОГ є слідчий, якого керівником органу досудового розслідування визначено здійснювати досудове розслідування кримінального правопорушення [143].

С. В. Чучко зазначає, що особи, які вчиняють шахрайства при купівлі-продажу товарів через мережу Інтернет, ведуть постійний обмін інформацією зі своїми жертвами. В основному таке спілкування здійснюється через мережу Інтернет. Крім того, для спілкування зі співучасниками, близькими особами й органами, які надають допомогу у реалізації умислу, застосовується здебільшого мобільний зв'язок. Для зібрання інформації стосовно їх спілкування необхідно проводити ряд негласних слідчих (розшукових) дій та оперативно-технічних заходів, пов'язаних зі

встановленням правопорушника та його зв'язків, наприклад, спостереження за об'єктом, прослуховування телефонних переговорів, огляд кореспонденції, зняття інформації з транспортних та електронних систем тощо. При цьому, найбільш типовими недоліками у взаємодії слідчих, оперативних працівників при вирішенні проблемних конфліктних слідчих ситуацій у справах про шахрайство у мережі Інтернет, є: несвоєчасний, із запізненням початок взаємодії. Адже необхідно починати взаємодію ще до відкриття кримінального провадження; здійснення затримання, огляду, допиту підозрюваних оперативними працівниками без участі слідчого або хоча б попереднього узгодження з ним шляхів і способів одержання та перевірки доказів причетності затримуваного до злочину; припинення взаємодії (особливо оперативного супроводу розслідування) після завершення початкового етапу досудового розслідування [205, с. 126].

Як зазначає М. В. Куратченко, до прийнятих на практиці заходів з усунення вказаних вище недоліків можна віднести:

– заходи щодо вдосконалювання нормативної та методичної бази взаємодії зазначених вище суб'єктів;

– перевірки дотримання діючих наказів та інструкцій з організації взаємодії на місцях, з виїздом керівників органів і служб у підлеглі підрозділи;

– заслуховування слідчо-оперативних груп, що працюють по конкретних справах і матеріалах, на оперативних нарадах у керівників управлінь і відділів;

– контрольне вивчення розслідуваних кримінальних проваджень про досліджувані види шахрайства начальниками слідчих підрозділів;

– вивчення справ прокурором у порядку нагляду[96].

У виявленні та розслідуванні кібершахрайств, вчинених в установах виконання покарань, важливою є комплексна співпраця працівників поліції зі співробітниками відділу протидії кіберзлочинам, оперативними

співробітниками слідчих ізоляторів та працівниками Департаменту з питань виконання кримінальних покарань Мін'юсту.

Як результат такої співпраці можна назвати викриття шахрая, який на платформах оголошень пропонував постачання генераторів з-за кордону. [124].

Як ми вже зазначали, шахрайство, пов'язане із електронною комерцією, все частіше стає об'єктом злочинної діяльності організованих злочинних угруповань, у тому числі й на транснаціональному рівні. Тому, в рамках організації розслідування шахрайства, пов'язаного з електронною комерцією, важливу роль займає міжнародне співробітництво із компетентними органами інших держав.

Наведемо приклад. Так, протягом 2019-2022 рр. злочинне угруповання використовувало скомпрометовані дані клієнтів іноземних банків для розрахунків в онлайн-магазинах. Куплені товари фігуранти перепродавали та одержували «прибутки». Кіберполіцейські разом зі слідчими, в рамках міжнародного співробітництва за участі правоохоронців Німеччини та Литви, за координації Офісу Генерального прокурора викрили 40-річного співорганізатора шахрайської схеми. Громадянин України спільно з громадянином Молдови організували схему шахрайського заволодіння грошовими коштами громадян Євросоюзу, до якої залучили вихідців з країн ЄС та ближнього зарубіжжя. Користуючись довірливим ставленням мешканців європейських країн до онлайн-покупок вони, попередньо заволодівши даними викрадених банківських карток, замовляли у мережі Інтернет товари на суму декілька тисяч євро за операцію. Оплачували товар за допомогою карток потерпілих осіб, а в подальшому, через спеціально організовану мережу торгових агентів, збували їх у східноєвропейських країнах. Транснаціональна злочинна група упродовж трьох років діяла на території ЄС та України, за цей період організаторам вдалося заволодіти грошовими коштами громадян ЄС на суму понад 600 тис. євро. В рамках кримінального провадження за ознаками злочину, передбаченого ч.3 ст. 190

КК України кіберполіцейськими Харківщини, за участі членів міжнародної слідчо-оперативної групи, проведено обшуки за місцем мешкання фігуранта та вилучено техніку, за допомогою якої вчинялись шахрайські дії. Фігуранта затримано прикордонниками Польщі за ордером на арешт від правоохоронних органів Німеччини, під час перетину кордону з Республікою Білорусь. Інший співорганізатор має статус обвинуваченого в рамках проведення розслідування поліцейськими Німеччини, де перебуває під вартою [192].

Під час застосовування положень з міжнародного співробітництва у кримінальному провадженні слідчі органи звертаючись через Офіс Генерального прокурора України до уповноваженого компетентного органу іноземної держави мають право робити запити у вигляді доручень, звернень щодо необхідності проведення окремих процесуальних дій (допит свідка, потерпілого, експерта, повідомлення про підозру, проведення обшуку, огляду, вилучення речей, документів, арешту чи конфіскації майна, проведення інших процесуальних дій), вручення документів, видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування тощо. До того ж, особливістю вказаного співробітництва є вимога щодо дотримання не лише положень чинного кримінального процесуального законодавства, але й дотриманням положень ратифікованих міжнародних правових актів з питань міжнародної правової допомоги у кримінальних провадженнях. А у випадку відсутності відповідного міжнародного договору, надання допомоги може здійснюватися на засадах взаємності (ст. 542, 544 КПК)[94]. За вказаним принципом правова допомога у кримінальному провадженні надається компетентним органом іноземної держави за умови, якщо направляючи до такої держави запит, Уповноважений центральний орган України (Офіс Генерального прокурора України) письмово гарантує запитуваній стороні розглянути в майбутньому її запит про надання такого самого виду міжнародної правової допомоги (ст. ч. 2 ст. 544 КПК) [63].

Отже, під час розслідування шахрайства в інтернет-комерції виникають різного роду організаційні питання, пов’язані із 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.

Запорукою успішного розслідування є також взаємодія слідчого із іншими правоохоронними органами 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 тощо).

В рамках організації розслідування шахрайства, пов’язаного з електронною комерцією, важливу роль займає міжнародне співробітництво із компетентними органами інших держав у вигляді надання запитів, звернень щодо необхідності проведення окремих процесуальних дій, вручення документів, видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування тощо.

2.3. Типові слідчі ситуації, що виникають під час досудового розслідування шахрайства в інтернет-комерції

У криміналістичній науці під час розробки окремих методик розслідування зазвичай вдаються до типізації слідчих ситуацій. Мета такої

типізації – створити й у подальшому практично застосувати типові комплекси слідчих (розшукових) дій, оперативно-розшукових заходів і тактичних операцій під час розслідування певного виду кримінального правопорушення. Виокремлення типових слідчих ситуацій розслідування є, передусім, продуктом наукового осмислення та має на меті сприяти оптимальній організації розслідування в аналогічних (тобто типових) ситуаціях. Знання слідчим певних «типів» ситуацій дає йому змогу: зорієнтуватися у всьому масиві інформації; висунути найбільш обґрунтовані версії й визначити (чи скоригувати) напрями їх перевірки; правильно обрати послідовність слідчих (розшукових) дій та оперативно-розшукових заходів тощо [79, с. 78]. Слідча ситуація як наукова криміналістична категорія має не тільки теоретичне, а, насамперед, прикладне значення для методики розслідування окремих видів злочинів [58, с. 118].

Як зазначає В. В. Логінова, слідча ситуація – це сукупність обставин, що сформувалась на певному етапі розслідування на підставі фактичних даних про подію злочину, яка обумовлює можливість органів досудового слідства реалізувати свої можливості щодо розкриття, розслідування та попередження злочину [101, с. 282].

Є. В. Пряхін термін «ситуація» трактує як сукупність умов та обставин, що створюють ті чи інші відносини, обстановку, стан; система зовнішніх щодо суб’єкта умов, які спонукають та опосередковують його активність [147, с. 75]. На думку С. В. Веліканова слідча ситуація – це сукупність сформованих на певному етапі умов – стану та обстановки розслідування, що сприймаються, оцінюються і використовуються слідчим для вирішення тактичних завдань і досягнення загальних (стратегічних) цілей розслідування [21, с. 9]. А вже В. А. Журавель при формуванні поняття типової слідчої ситуації визначає її як наукову абстракцію, своєрідну інформаційно-пізнавальну модель, що сформована на підставі апріорних знань, яка є результатом узагальнення й аналізу значного емпіричного

матеріалу і в якій відображені найбільш загальні риси, що характеризують хід і стан розслідування на певному етапі (початковому, наступному) [59, с. 202].

Аналізуючи визначення «слідчої ситуації», можна сказати, що вчені під поняттям «ситуація» розуміють комбінацію факторів, доказової та іншої інформації, якою володіють слідчі в певний момент розслідування або перед його початком [40, с. 302].

Натомість, на думку Р. Л. Степанюка, поняття типової слідчої ситуації не варто обмежувати тільки даними про сукупність наявної в слідчого інформації про обставини злочину, а доцільно включати й інший інформаційний компонент – про найбільш значущі характеристики процесу розслідування [172, с. 111].На цьому наполягає й М. С. Качковський, який наголошує на тому, що типізація слідчих ситуацій можлива за умови виділення інформації про окремі найбільш значущі елементи і таких компонентів, що часто зустрічаються. Втім, окрім відомостей про окремі обставини злочинної діяльності (особу, яка вчинила злочин, спосіб, сліди злочину, предмет посягання і розмір заподіяної злочином шкоди, зв’язки з іншими злочинами), слід враховувати ще й сукупність інформації про найбільш значущі обставини розслідування (стан доказової бази, можливості слідства, лінія поведінки підозрюваних та інших учасників розслідування, сторонніх осіб, які намагаються втручатися у процес розслідування тощо) [69].

І. В. Калініна типову слідчу ситуацію визначає як об’єктивні положення, що виникають, в першу чергу, на початковому етапі розслідування на базі незначного обсягу інформації і часто повторюються у практиці розслідування. Інформація про типові слідчі ситуації є результатом узагальнення практики розслідування певного виду злочинів [67, с. 215].

Є ряд наукових праць, в яких проблеми слідчих ситуацій висвітлюються у двох ракурсах. Так, Т. А. Пазинич вважає, що використовуване в криміналістиці поняття слідчої ситуації є узагальненим і фактично охоплює два поняття: «конкретна слідча ситуація у кримінальному провадженні» та

«типова слідча ситуація», де конкретна слідча ситуація – це сукупність всіх умов, в яких здійснюється розслідування в певний його момент. Типова слідча ситуація – це сукупність інформації (доказів та оперативно-розшукових відомостей), яка найбільш характерна для певного етапу розслідування у кримінальних провадженнях окремих категорій [131, с. 126].В. Ю. Шепітько слідчу ситуацію також розглядає в широкому і вузькому розумінням. У широкому розумінні слідча ситуація являє собою сукупність усіх умов, що впливають на розслідування і визначають його особливості. Така сукупність найповніше характеризує і відображає усе, що впливає і може впливати на розслідування злочину, а відтак, дає змогу вичерпно визначити шляхи і засоби цілеспрямованого впливу на сформовану слідчу ситуацію [93, с. 97].

Як показав аналіз юридичної літератури, широку підтримку та подальший розвиток в наукових колах одержало визначення, що запропоноване В. П. Бахіним, який слідчу ситуацію визначив як об’єктивну реальність, фактичну обстановку, а результат її пізнання, відомості про неї – відображенням цієї обстановки, що використовуються для з’ясування її змісту з метою розкриття кримінального правопорушення та притягнення винних осіб до відповідальності [168, с. 16; 134].

Отже, можна дійти висновку, що думки вчених щодо слідчої ситуації, як і стосовно будь-якої криміналістичної категорії, різняться між собою.

Зокрема, одні вчені формулюють слідчу ситуацію як сукупність фактичних даних, які відображають подію, що розслідується. Інші вчені у слідчій ситуації бачать інформаційну модель, динамічну інформаційну систему, що містить ознаки, які мають значення у кримінальній справі. Треті вчені вважають, що слідча ситуація – це сукупність даних, за яких слідчий повинен діяти. Слідча ситуація – це обстановка, картина розслідування, яка склалася на певний момент розслідування, тобто сума значущої інформації. Четверті вчені визначають слідчу ситуацію як сукупність умов, в яких на

певний момент здійснюється розслідування, тобто обстановку, в якій проходить процес розслідування [85, с. 139; 78, с. 185].

Проте, в одному всі абсолютно мають одностайні думки – вирішення тактичних завдань і досягнення цілей розслідування є можливим тільки завдяки визначенню та оцінки слідчої ситуації.

Аналіз і оцінка слідчої ситуації мають істотне значення, тому що дозволяють:

– зорієнтуватися у всьому розмаїтті фактів і явищ, які відносяться до особи злочинця на даний момент розслідування;

– усвідомити наукові знання (рекомендації криміналістики) щодо типових матеріальних джерел (слідів), у яких відбувається подія злочину;

– опанувати методики та практики пошуку таких джерел, отримати від них належну інформацію, її фіксація та подальше збереження;

– виконувати практичну роботу з цими джерелами інформації;

– співставляти отриману інформацію з даними оперативних і криміналістичних обліків;

– висунути відповідні версії про місцезнаходження і сліди, що містять інформацію про властивості особи злочинця;

– визначити найбільш доцільні тактичні прийоми, рекомендації, комбінації зі збирання слідів для встановлення злочинця;

– вибрати найбільш ефективні техніко-криміналістичні засоби і методи для цих цілей;

– вибрати найбільш ефективні форми використання спеціальних знань і взаємодії з органами дізнання з метою одержання криміналістично значущої інформації про особу злочинця;

– спланувати початковий етап розслідування [58, с. 121].

Слід сказати, що виділення слідчих ситуацій, що виникають при розслідуванні шахрайств, пов’язаних із електронною комерцією, потребує визначення певних критеріїв, на яких здійснюватиметься їх типізація.

З урахуванням вищеперерахованого, Л. Г. Дунаєвська та Я. С. Маркевич сформували перелік найбільш типових критеріїв слідчих ситуацій, що виникають при розслідуванні даного виду злочинів.В залежності від етапу розслідування: слідча ситуація, що виникла на початковому етапі; слідча ситуація, що виникла на наступному етапі. Водночас, в залежності від джерела надходження інформації щодо кримінального правопорушення: повідомила потерпіла особа; повідомили родичі чи близькі потерпілої особи; повідомили особи, з якими потерпілий проживає; повідомлення засобів масової інформації; стало відомо під час розслідування іншого злочину. Разом з тим, залежно від складності слідчої ситуації: проста слідча ситуація – відомо про факт вчинення злочину, відома особа, яка його вчинила або про неї є орієнтовна інформація, відома потерпіла особа; складна слідча ситуація: а) відомо про факт вчинення злочину, відома потерпіла особа, не відома особа, яка вчинила злочин; б) відомо про факт вчинення злочину, особа потерпілого не встановлена, не відома особа, яка вчинила злочин; в) відомо про факт вчинення злочину, відома особа, яка вчинила злочин, особа потерпілого не встановлена. Залежно від позицій сторін кримінального провадження: безконфліктна – особа, що вчинила злочин, відома, визнає свою вину та сприяє розслідуванню; конфліктна – особа, що вчинила злочин, вини не визнає, особа, що володіє інформацією, не бажає її повідомити, або повідомляє умисно неправдиву інформацію[49, с. 127].

Аналіз криміналістичній літератури показав, що деякі вчені намагалися сформувати слідчі ситуації розслідування шахрайств, вчинених у мережі Інтернет.

Першим намагався досягти результатів у цьому напрямі С. В. Самойлов, який виокремив три типові слідчі ситуації, які мають місце на початковому етапі розслідування шахрайств, вчинених з використанням мережі «Інтернет»:

Ситуація 1. Виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця або встановлено, або

достатньо даних для її встановлення.

Ситуація 2. Виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено, однак є певні відомості, що можуть вказувати на неї. Ситуація

Ситуація 3. Виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї [158, с. 26; 157].

С. В. Чучко Аналіз судово-слідчої практики дозволив нам сформулювати типові слідчі ситуації розслідування досліджуваного виду шахрайства, зокрема:

1) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, наявна особистісна доказова інформація, злочинець відомий – 34 %;

2) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, наявна особистісна доказова інформація, злочинець невідомий – 41 %;

3) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, наявна матеріальна й особистісна доказова інформація, злочинець невідомий – 17 %;

4) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, відсутня достатня доказова інформація – 8 %.

До кожної з наведених ситуацій наведемо алгоритм можливих дій. Так, у першій ситуації (наявна особистісна доказова інформація, злочинець відомий) уповноважена особа повинен провести НСРД для документування спілкування шахраїв, їх дій. Крім того, необхідно здійснити додаткові допити потерпілих і свідків з метою додаткової фіксації шахрайських дій і мотивів шахраїв.

У другій ситуації (наявна особистісна доказова інформація, злочинець невідомий) обов’язковим є встановлення злочинця, а також його зв’язків.

У третій ситуації (наявна матеріальна й особистісна доказова інформація, злочинець невідомий) необхідно проводити одночасні допити

між потерпілими та свідками з приводу виявлення, усунення протиріч у їх показаннях.

Для четвертої ситуації (відсутня достатня доказова інформація) найбільш характерним є здійснення заходів щодо фіксації дій шахрая [205, с. 125].

Т. В. Коршикова умовно виокремила дві основні групи типових слідчих ситуацій на початковому етапі розслідування шахрайства з використанням ЕОТ, обравши критерій поділу «залежно від характеру первинної інформації про подію та її учасників» [81, с. 110].

Говорячи про утворення типових слідчих ситуацій під час розслідування шахрайства при розслідуванні кіберзлочинів, слід звернути увагу на науковий підхід О. А. Самойленко, яка критерієм їх розподілу обрала джерело інформації про факт вчинення кіберзлочинів:

- потерпілий самостійно запідозрив вчинення незаконних дій у кіберпросторі та одразу звернувся до відповідного оперативного підрозділу кібеполіції, слідчого або прокурора, також сам діагностував сліди (зміни у файловій системі, в заданій раніше конфігурації комп'ютера, нестандартні прояви в його роботі тощо в залежності від ситуації);

- шахрайство виявлено у результаті проведення перевірочних заходів співробітниками служби безпеки або фахівцями із захисту інформації, що знаходяться в штаті користувача або провайдера (наприклад, при перевірки службою безпеки банка виявляються сліди вчинення кіберзлочину) [154, с. 24].

В контексті даної проблематики О. В. Ковальчук та Є. В. Пряхін також відстоюють позицію, що розподіл слідчих ситуацій пов'язаний не лише з обсягом, а й з характером джерел початкової інформації про злочин на стадії відкриття кримінального провадження.

З огляду на це можна вирізнити кілька типових слідчих ситуацій початкового етапу розслідування шахрайства:

1. Кримінальне провадження розпочато на підставі матеріалів, зібраних за результатами проведення спеціальних (планових чи позапланових) перевірок або з інших гласних джерел (повідомлень потерпілих, свідків). Особливістю цієї ситуації є те, що вихідна інформація зазвичай міститься у матеріалах: – документальної перевірки (податкової, банківської, ревізійної та ін.), під час якої виявлено ознаки шахрайства; – судового розгляду позовів у порядку господарського судочинства; – оприлюднених у ЗМІ (наприклад, журналістському розслідуванні). Факторами, що можуть негативно впливати на розслідування у вказаній ситуації, є: відсутність раптовості, тобто шахрай чи інші зацікавлені особи, як правило, знають про перевірку та виявлені факти шахрайства; істотний розрив у часі з моменту вчинення шахрайства до його виявлення, що дає змогу вжити заходів для знищення слідів шахрайства.

2. Кримінальне провадження розпочинається з реалізації матеріалів, зібраних оперативними підрозділами. Такі матеріали заводяться на підставі: заяв громадян про; результатів проведення оперативно-розшукових заходів під час оперативного обслуговування об’єктів фінансової системи. Цю ситуацію можна назвати найсприятливішою з точки зору перспектив розслідування, оскільки негласний характер перевірки, по-перше, дає змогу виявити широке коло обставин протиправної діяльності, а по-друге, припускає здійснення добре запланованого, несподіваного для шахрая, одночасного проведення низки оперативно-розшукових заходів та процесуальних дій у формі тактичних операцій.

3. Кримінальне провадження розпочато під час розслідування іншого кримінального правопорушення. Практика діяльності правоохоронних органів свідчить про те, що ознаки шахрайства можуть бути виявлені в процесі розслідування, скажімо, кримінальних правопорушень у сфері господарської діяльності. У такому разі кримінальне провадження розпочинається на підставі письмового рапорту слідчого. Позитивним є те, що у розпорядженні органів досудового розслідування вже є значна кількість документів, оскільки вони зібрані в ході першого кримінального

провадження. До речі, керуватися потрібно нормами ст. 217 КПК України, де вказано, що рішення про виділення матеріалів провадження на стадії досудового розслідування приймає прокурор. Виділення матеріалів з одного або кількох кримінальних правопорушень можливе за умови, що це негативно не вплине на повноту досудового розслідування та судового розгляду [79, с. 80-81 ; 94].

В контексті даної проблематики імпонує підхід Н. В. Павлової, Д. А. Птушкіна та К. О. Чаплинського, які критеріями для визначення слідчих ситуацій шахрайства обрали«наявність елементів процесуального і тактичного характеру» та «наявність елементів матеріального та організаційно-технічного характеру» [126].

Дані критерії цілком ймовірно можна покласти в основу формування слідчих ситуацій початкового етапу розслідування шахрайств, пов’язаних із електронною комерцією.

Зокрема, за процесуально-тактичним характером можна визначити такі слідчі ситуації: підозрюваного затримано, йому повідомлено про підозру, до нього обрано захід запобігання. Умови для проведення всіх можливих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших організаційних заходів є сприятливими; підозрюваного затримано, повідомлено про підозру, до нього обрано захід запобігання, але умови для проведення всіх можливих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших організаційних заходів є несприятливими (відмова від участі у слідчому експерименті, недостатньо підстав для проведення обшуку, знищення зацікавленими особами документів, щодо яких планувалося проведення експертиз тощо); підозрюваного затримано, повідомлено про підозру, до нього обрано захід запобігання, але є достатні підстави вважати, що шахрайство вчинене у співучасті з іншими особами, інформація щодо яких відсутня; особа (особи), яка (які) вчинила (вчинили) шахрайство встановлена (встановлені), але наявні факти не надають

достатніх підстав для повідомлення підозри та обрання заходу запобігання [126].

Натомість, опитування респондентів показало, що в основному загальноприйнятним є підхід до визначення слідчих ситуацій, згідно якого обираються напрями розслідування саме за характером наявної інформації.

Зокрема, при розслідуванні шахрайств, пов'язаних з електронною комерцією, слідчі виділяють такі слідчі ситуації:

1) наявна інформація про особу шахрая та механізм вчинення шахрайства в цілому (57 %);

2) наявна інформація про обставини вчинення шахрайства, але дані про шахрая невідомі, натомість, є вірогідність їх встановлення (13 %);

3) є інформація про обставини вчинення шахрайства, але особистості злочинців невідомі (30 %).

Перша слідча ситуація передбачає проведення комплексу заходів, спрямованих на встановлення всіх обставин справи та доведення вини особи, яку підозрюють у вчиненні шахрайства в інтернет-комерції, зокрема: допиту потерпілого щодо обставин здійснення правочину у дистанційній формі та умов, які висувалися продавцем та покупцем; встановлення умов створення сайту, на якому викладалися пропозиції щодо купівлі-продажу товарів та послуг; отримання інформації від інтернет провайдерів та операторів телекомунікаційного зв'язку; допиту підозрюваного щодо обставин ошукування громадян, легітимності існування його діяльності тощо; отримання характеризуючих даних про підозрюваного; пред'явлення підозрюваного для впізнання потерпілому (за умов спілкування в відео-режимі); огляд засобів комп'ютерної техніки, проведення обшуку у підозрюваного тощо; призначення комп'ютерно-технічної та інших експертиз тощо.

У ситуації, коли особи шахраї не переховуються від правоохоронних органів, але свою причетність до вчинення шахрайства заперечують, перед слідчим постають завдання щодо необхідності виявлення, зібрання, та

отримання певної сукупності, належних, обґрунтованих, та достатніх обвинувальних доказів, шляхом з'ясування у потерпілих осіб всіх обставин, за яких розпочиналися та завершилися шахрайські дії, і роль кожної причетної (підозрюваної) до цього особи, здійснення детального огляду місця події, вилучення слідів, які вказують на факт шахрайства. Встановлення можливих його свідків. Проведення впізнання осіб причетних до шахрайських дій, термінове проведення обшуків житла та іншого їх володіння, з метою вилучення електронних носіїв, та інших документів і предметів, які свідчать про вчинення шахрайських дій. Для покращення результативності розслідування доцільно проводити й негласні слідчі (розшукові) дії з метою встановлення злочинних зв'язків шахрая, його образу життя, можливого місця знаходження, речей предметів, документів, що підтверджують причетність до шахрайства та інших доказів, які цікавлять слідство [63].

У другій слідчій ситуації, коли наявна інформація про обставини вчинення шахрайства, але дані про шахрая невідомі, натомість, є вірогідність їх встановлення, окрім вказаних вище заходів, всі зусилля повинні спрямовуватися на отримання інформації щодо місцезнаходження шахрая.

Для цього, слід докладно допитати потерпілого та свідків щодо прикмет особи, яка вчинила шахрайство, скласти та поширити орієнтування, повідомити інформацію про злочинця у засоби масової інформації тощо. Інформацію про місцезнаходження шахрая можуть надати його знайомі та родичі, співробітники та інші особи. Оперативним працівникам можна здійснити спостереження за місцями можливої появи шахрая та, у разі необхідності, здійснити зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем. Втім, слід пам'ятати, що дані заходи є негласними слідчими (розшуковими) діями і проводитися можуть за дорученням слідчого і тільки на підставі ухвали слідчого судді (за умов вчинення злочину, а не проступку). Якщо шахрайство кваліфікуватиметься за ч. 1 ст. 190 КК України, це буде кримінальний

проступок і серед всіх НСРД можна проводити тільки дві: встановлення місцезнаходження радіоелектронного пристрою та зняття інформації з електронних інформаційних систем (без порушення системи логічного захисту). Докази щодо дійсного злочинного наміру можна отримати не лише зі свідчень потерпілих, та свідків обставин шахрайських дій, але й під час огляду документів, електронних інформаційних носіїв, уважно оглядаючи відповідні інформаційні ресурси, сервіси в мережі Інтернет, у тому числі веб-сайти, на яких міститься інформація, що може допомогти довести дійсно злочинний намір шахраїв. З цією метою, доцільно проводити й негласні слідчі (розшукові) дії знімаючи необхідну інформацію з каналів зв'язку [63].

У третій ситуації, коли особистість шахрая невідома, проводиться комплекс розшукових заходів з використанням словесного та композиційного портретів тощо. Зі слів потерпілих та свідків за прикметами шахраїв складаються суб'єктивні портрети, перевіряються за обліками сліди пальців рук, виявлені на документах та предметах. Корисним може бути й вивчення практики застосування аналогічних способів шахрайства за архівними кримінальними справами (провадженнями) [126, с. 65].

У цій ситуації доцільно також застосувати методи цифрової криміналістики. Як зазначає Р. Л. Степанюк, засоби і методи цифрової криміналістики широко застосовуються в оперативно-розшуковій діяльності з метою виявлення ознак кримінального правопорушення, на стадії досудового розслідування при підготовці та проведенні негласних і гласних слідчих (розшукових) дій, пов'язаних зі збиранням цифрових доказів, у судовій експертизі комп'ютерної техніки та програмних продуктів та в інших експертизах, які досліджують цифрові докази [223; 170, с. 288].

Зокрема, слід спрямувати всі сили на дослідження:операційної системи та оперативної пам'яті; вивчення змісту файлів; web-браузерів; вивчення змісту електронної пошти; вивчення змісту смс повідомлень, журналу вхідних та вихідних дзвінків на мобільному пристрої потерпілого тощо.

У будь-якій слідчій ситуації, визначаючи напрями розслідування, слід враховувати, що типовими джерелами доказів у кримінальних провадженнях про шахрайства даної категорії можуть виступати:

- показання потерпілого щодо обставин вчинення злочину;

- показання свідків з числа осіб близького оточення потерпілого щодо обставин вчинення злочину;

- зміст листування між шахраєм і потерпілим (дані вилучених скріншотів);

- дані щодо одночасного листування шахрая з іншими потенційними жертвами;

- квитанції про перерахування коштів потерпілим на рахунки шахрая;

- квитанції про зняття з рахунків готівки, що потім передавалась шахраю;

- кредитні договори та боргові розписки, що підтверджують факт отримання коштів потерпілим для розрахунків з шахраєм;

- виписки по рахунках, що належать шахраю, про рух коштів по його банківським карткам;

- факт користування підслідним сторінками в соціальних мережах від імені вигаданих осіб;

- факт впізнання потерпілим підслідного за ознаками голосу, якщо мали місце телефоні перемовини;

- факт належності підслідному віш-карти, за допомогою якої здійснювались дзвінки потерпілому;

- притягнення затриманого раніше до кримінальної відповідальності за вчинення аналогічних злочинів;

- факт відсутності законних джерел прибутку у підслідного, при наявності в нього значних грошових коштів, джерело отримання яких він не може пояснити [66, с. 76].

Отже, для успішного планування розслідування шахрайств в інтернет-комерції, насамперед необхідно визначити типову слідчу ситуацію,

що склалася на певному етапі розслідування, та окреслити першочергові завдання, які необхідно вирішити.

Висновки до розділу 2

Констатуючи сказане у розділі, спробуємо підсумувати зазначене таким чином.

1. Успіх розслідування залежить від того, наскільки правильно слідчий (дізнавач) зорієнтується в тій чи іншій ситуації та визначить заходи, які є найбільш ефективними та результативними. 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 кримінальних правопорушень 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 кримінального провадження (у зв’язку з відсутністю складу злочину, або встановленням неможливості виконати цивільно-правові зобов’язання у зв’язку з форсмажорними обставинами).

2. Ефективність і якість 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 кримінальних правопорушень на різних етапах розслідування.

3. Однією з умов вчасного запобігання шахрайським проявам, швидкого розкриття й розслідування шахрайств в інтернет-комерції є правильна організація взаємодії відповідних органів. На підставі цього визначено напрями взаємодії органів Національної поліції України 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.

У виявленні та розслідуванні кібершахрайств, вчинених в установах виконання покарань, важливою є комплексна співпраця працівників поліції з оперативними співробітниками слідчих ізоляторів та працівниками Департаменту з питань виконання кримінальних покарань Мін'юсту.

4. В рамках організації розслідування шахрайства, пов'язаного з інтернет-комерцією, 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 кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування та ін.

5. 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 особу шахрая і механізм учинення шахрайства в цілому) передбачається проведення комплексу заходів, спрямованих на встановлення усіх обставин справи та доведення вини особи, яку підозрюють у шахрайстві в інтернет-комерції, зокрема: допит потерпілого щодо обставин здійснення правочину у дистанційній формі та умов, які висувалися продавцем і покупцем; встановлення умов створення сайту, на якому викладалися пропозиції щодо купівлі-продажу товарів і послуг; отримання інформації від інтернет-провайдерів та операторів телекомунікаційного зв'язку; допит підозрюваного щодо обставин ошукування громадян, легітимності існування його діяльності; отримання характеризуючих даних про підозрюваного;

пред’явлення підозрюваного для впізнання потерпілому (за умов спілкування в відеорежимі); огляд засобів комп’ютерної техніки, проведення обшуку у підозрюваного; призначення комп’ютерно-технічної та інших видів експертиз. У другій слідчій ситуації, коли наявна інформація про обставини учинення 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 злочинця 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.

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО-ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ ШАХРАЙСТВА ВІНТЕРНЕТ-КОМЕРЦІЇ

3.1. Організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій

Процесуальний зміст слідчих (розшукових) дій визначено у главі 20 КПК України. При цьому, підставами для проведення слідчої (розшукової) дії є наявність достатніх відомостей, що вказують на можливість досягнення її мети [36, с. 63].

У кримінальних провадженнях щодо шахрайств в інтернет-комерції ставиться ряд завдань, більшість з яких можна вирішити через проведення слідчих (розшукових) дій, а за тяжкими та особливо тяжкими злочинами – у тому числі шляхом проведення негласних слідчих (розшукових) дій.

Як показав аналіз судово-слідчої практики, у кримінальних провадженнях щодо шахрайств в інтернет-комерції, здебільшого проводяться такі слідчі (розшукові) та негласні слідчі (розшукові) дії:допит (100 %); проведення допиту в режимі відео конференції (23 %); пред’явлення особи для впізнання (8 %); пред’явлення особи для впізнання в режимі відео конференції (13 %);пред’явлення речей для впізнання (11 %); обшук (56 %); огляд (92 %); слідчий експеримент (5 %); проведення експертизи (100%); отримання зразків для експертного дослідження (91 %).

Крім того, у вказаних провадженнях у 98 % випадках проводиться такий захід забезпечення кримінального провадження, як тимчасовий доступ до речей та документів.

Процентне відношення вказаних процесуальних дій свідчить про те, що серед них найпоширенішими є допит, обшук, огляд, тимчасовий доступ до

речей та документів, проведення експертизи. Серед негласних слідчих (розшукових) дій найчастіше проводяться: зняття інформації з електронних комунікаційних мереж (76 %); зняття інформації з електронних інформаційних систем (75 %); установлення місцезнаходження радіообладнання (радіоелектронного засобу) (91 %) тощо.

Тому пропонуємо приділити увагу саме специфіці вказаних процесуальних дій і розпочати з тих, що спрямовані на одержання інформації з матеріальних джерел (огляду, обшуку, тимчасовому доступу до речей та документів). Дана необхідність викликана тим, що у ході розслідування таких кримінальних правопорушень виникає необхідність у виявленні, фіксації та вилученні ряду об’єктів, що мають доказове значення. До того ж, процес вчинення шахрайства в інтернет-комерції пов'язаний із використанням низки документів (паперових та електронних), які відображають інформацію про здійснений правочин, та здійсненням ряду операцій, які відбуваються через електронні та телекомунікаційні мережі. З однієї сторони, одержана інформація може сприяти встановленню ряду фактів щодо здійснення правочину, з іншої – паперові та електронні документи, а також комп’ютерна техніка тощо можуть виступати речовими доказами у провадженні.

Слід сказати, що розвиток цифрових технологій зумовлює вилучення окрім традиційних об’єктів ще й інформаційних слідів, які утворюються внаслідок впливу на комп’ютерну інформацію (шляхом знищення, перекручення). Насамперед вони залишаються на магнітних носіях інформації і пов’язані зі змінами, які відбулися у самій інформації, порівняно з початковим її станом. Також до інформаційних слідів належать наслідки роботи антивірусних і тестових програм, які можуть бути виявлені під час вивчення комп’ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм та програмного забезпечення [133, с. 8].

Під час обшуків та тимчасового доступу до речей та документів у

справах щодо шахрайства вилучаються й велика кількість матеріальних об’єктів: рукописні записи та схеми і графіки про злочинні дії у записних книжках та на окремих аркушах (14 %); роздруківки із криміналістично значимою інформацією (6 %); взуття, одяг, аксесуари, засоби маскування (перуки, вуса, накладні носи та ін.) (17 %); бланки документів, які необхідні для здійснення шахрайських дій (67 %); спеціальна література (на тему підробки документів, психології обману, правил укладання угод) (11 %); виписки із журналів із інформацією про об’єкти нерухомого майна та їх власників (5 %); газети із підкресленням номерів телефонів (3 %); різноманітні заяви, що подаються шахраєм до органів, які мають відношення до здійснення операцій з нерухомості (4 %); печатки та штампи як справжні (шахраї нерідко викрадають їх для використання у злочинних цілях), так і підроблені (36 %); кліше підписів (18 %); документи, що посвідчують особистість (паспорти, посвідчення тощо яксправжні, так і підроблені) (54 %). Матеріальні сліди також можуть залишатися на обчислювальній техніці (сліди від пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо), а також на магнітних носіях і оптичних дисках [148].

Вказані об’єкти можна вилучити шляхом тимчасового доступу до речей та документів у разі, якщо йдеться про добровільну видачу речей та документів, які знаходяться у володінні певної особи. До таких осіб можна віднести: представників банківської установи, інтернет-провайдерів, власників комп’ютерних клубів та інтернет-кафе та ін.

Натомість, іноді особи, у володінні яких знаходилися речі та документи, що мають значення для справи, відмовляють у наданні доступу до них. За таких обставин слідчі вимушені переключатися на примусове вилучення вказаних об’єктів. Нерідко слідчі відразу приймали рішення про проведення обшуку, оскільки розуміли про неможливість добровільної видачі таких об’єктів. До того ж, нерідко виникає необхідність діяти раптово, із метою унеможливлення знищення об’єктів, що мають значення для справи, а також досягнення інших тактичних завдань, наприклад: з метою відшукування у

житлі злочинця, виявлення і вилучення предметів і цінностей, здобутих злочинним шляхом або тих, що були знаряддям злочину, для забезпечення відшкодування збитків, завданих кримінальним правопорушенням тощо [82].

Маємо констатувати, що у 56 % випадків під час розслідування шахрайств в інтернет-комерції виникає необхідність саме примусового вилучення, тобто, шляхом обшуку. Проведення цієї слідчої (розшукової) дії потребує ретельної підготовки та продумування тактики дій.

Від того, як слідчий продумає всі деталі подальшого обшуку, залежить його успішність.

Тому важливе значення має правильне обрання підготовчихзаходів обшуку, до яких здебільшого відносяться: вивчення матеріалів кримінального провадження; збір орієнтуючої інформації про: особу злочинця, а також членів його сім'ї, родичів та знайомих; структуру та склад ЗУ; усі епізоди організованої злочинної діяльності; місця (об'єкти) обшуків; знаряддя (засоби) злочину та предмети, що здобуті злочинним шляхом і підлягають відшуканню тощо; аналіз й оцінка зібраної інформації та слідчої ситуації, що склалася на певному етапі розслідування, до ухвалення рішення про проведення обшуків; прийняття (ухвалення) рішення про проведення одночасних обшуків; планування та визначення часу проведення обшуків; створення оптимальних умов для проведення даної слідчої (розшукової) дії; визначення та підготовка необхідних транспортних, науково-технічних та інших спеціальних засобів (озброєння); добір необхідних учасників для проведення одночасних обшуків; визначення способу фіксації ходу та результатів обшуків; розробка заходів, що передбачають дії учасників обшуку у випадках виникнення не передбачуваних ситуацій або ускладнень; складання плану проведення одночасних обшуків; проведення інструктивної наради серед усіхучасників слідчої дії [198].

Натомість, як показав аналіз судово-слідчої практики та опитування респондентів, під час обшуку у провадженнях щодо шахрайства, пов'язаного з інтернет-комерцією, виникає проблема щодо встановлення попереднього

переліку об’єктів, які підлягають вилученню.

Як справедливо зазначає Н. В. Павлова, не дивлячись на вимогу кримінального процесуального законодавства (п. 7 ст. 234 КПК) вказувати в ухвалі на проведення обшуку всіх індивідуальних або родових ознак речей, документів, іншого майна або осіб, яких планується відшукати, а також їхнього зв’язку із вчиненим кримінальним правопорушенням, у більшості матеріалів кримінальних проваджень ці ознаки вказуються вельми розпливчасто та не в повному обсязі. Слідчі, дізнавачі пояснили такий підхід недостатністю інформації щодо об’єктів пошуку на момент прийняття рішення про проведення обшуку. До того ж, вони не вбачають проблеми вилучити майно, не вказане в ухвалі, оскільки за правилами п. 7 ст. 236 КПК України таке майно вважається тимчасово вилученим. Натомість на практиці виникає низка питань, пов’язаних із процедурою повернення такого тимчасово вилученого майна. До того ж, особи, в яких проводилися обшуки, та їх захисники нерідко вбачають у таких діях порушення їхніх прав і свобод [130, с. 280].

На підтвердження можна навести приклад із судової практики. Так, під час проведення обшуку було тимчасово вилучено речі, котрі належать ТОВ «ОСОБА_3». Відповідно до ухвали слідчого судді, дозвіл на проведення обшуку було надано слідчому з метою виявлення і вилучення документів і предметів, що свідчать про фінансово-господарські операції товариства з обмеженою відповідальністю – посадових інструкцій посадових осіб, чорнових записів, комп’ютерної техніки (CD, DVD дисків, флеш-накопичувачів, жорстких дисків та ін.), печаток вказаних та інших підприємств, мобільних телефонів, факсиміле. Втім, в ухвалі слідчого судді про дозвіл на проведення обшуку надано дозвіл на вилучення комп’ютерної техніки та конкретизовано, що комп’ютерна техніка – це CD, DVD диски, флеш-накопичувачі, жорсткі диски та ін., однак прямо не вказано щодо надання дозволу на вилучення ноутбуків. Ноутбуки не були отримані в результаті вчинення кримінального правопорушення, не є засобами або

знаряддями його вчинення, слідчим не було повідомлено, що інформація, яка міститься на вказаній комп'ютерній техніці, є необхідною умовою проведення експертного дослідження, доступ до даної комп'ютерної техніки не обмежувався адвокатом під час проведення обшуку, а навпаки, неодноразово слідчому пропонувалось здійснити копіювання інформації з такої техніки, та системи логічного захисту на вищевказаних інформаційних системах не знаходилось, що надавало змогу слідчому безперешкодно скопіювати інформацію з ноутбуків. Ці ноутбуки є тимчасово вилученим майном та потребували накладення арешту, однак слідчий не звернувся до слідчого судді з відповідним клопотанням і не повернув майно власнику, що зумовило ряд скарг з боку адвокатів [130; 163].

Як показав аналіз судово-слідчої практики та опитування респондентів, під час обшуку у провадженнях щодо шахрайства, пов'язаного з інтернет-комерцією, вилученню підлягають такі об'єкти: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 та авіа квитків, туристичних полісів тощо (12 %); документи, що підтверджують виконання договірних зобов'язань (12 %); документи, що підтверджують оплату послуг (розрахунковий документ) (43 %); договори між організаціями та 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 (застосовувалися при онлайн-спілкуванні) (8 %) тощо.

З цього виходить, що у досліджуваній категорії проваджень питому вагу вилучень складає саме комп'ютерна техніка, технічні засоби телекомунікації, а також програмне забезпечення.

Отже, слідчий стикається із рядом задач технічного та програмного характеру, які потребують втручання обізнаних осіб.До того ж, злочинці нерідко використовують технології захисту комп'ютерної інформації (56 %) – аутентифікацію конкретного користувача, засоби архівації на спеціалізованому сервері, криптографічний захист інформації та ін. [83, с. 16], що також потребує використання спеціальних знань.

Згідно ст. 15 Закону України «Про електронну комерцію», якщо законом або договором між сторонами визначено строк зберігання окремих видів документів, пов'язаних з вчиненням електронного правочину, сторони зобов'язані забезпечити архівне зберігання таких електронних документів (повідомлень), програмних, апаратно-програмних, апаратних або інших засобів для їх зберігання, в яких вони зберігаються і за допомогою яких можна відобразити інформацію, що в них міститься.Зберігачем електронних документів може бути суб'єкт господарювання, який надає послуги із зберігання електронних документів (повідомлень) шляхом забезпечення їх цілісності та незмінності за допомогою інформаційно-комунікаційних систем [142]. До цього архіву знову ж таки необхідний доступ.

Найбільш доцільним у провадженнях щодо шахрайств в інтернет-комерції є залучення фахівцівз комп'ютерної техніки та програмного забезпечення (програміст, системний інженер та ін.).

Ряд науковців стверджують, що залученням спеціалістів до проведення обшуку можуть досягатися різні цілі: застосування науково-технічних засобів, зокрема, пошукових приладів; застосування складних технічних засобів для фіксації ходу і результатів обшуку; розпізнання дійсної сутності тих чи інших предметів;одержання консультацій з питань дотримання правил безпеки[187, с. 321].

Окрім допомоги у дослідженні інформації, спеціаліст також вживає заходів для її перенесення на зовнішні носії інформації після визначення відношення інформації до розслідуваної події. При огляді документів, які можуть мати значиму для провадження інформацію, звертається увага на робочі записи співробітників, що працюють з комп'ютером. При складанні протоколу обшуку спеціаліст допомагає слідчому в описі виявлених об'єктів, місць, де вони були знайдені, дій по роботі з науково-технічними засобами [187, с. 323].

В розрізі цієї проблематики, слід зазначити, що О. А. Самойленко сформувала достатньо чіткий алгоритм дій під час огляду локального комп’ютерного засобу, зокрема:

- після вмикання комп’ютера необхідно пересвідчитись у налаштуванні BIOS на завантаження з приводу оптичних дисків або з флеш-накопичувача (при загрузці натиснути клавішу Del, Esc або F2 – при включенні, у разі потреби внести необхідні зміни та перезавантажити);

- завантажити операційну систему з робочого примірника спеціаліста;

- підключити принтер, роздрукувати текст із правами й обов’язками учасників слідчої дії, ознайомити їх із цими документами під підпис;

- приєднати носій, на який здійснюватиметься запис і на якому зберігатиметься інформація, отримана під час огляду, після чого його від форматувати;

- за допомогою відповідної програми вивести на екран монітора інформацію про апаратне та програмне забезпечення комп’ютера, необхідну для його ідентифікації, зберегти її як окремий файл;

- у разі потреби в перегляді файлів із відеограмами запустити програму запису зображення екрана монітора;

- здійснити огляд вмісту носіїв інформації, демонструючи учасникам зміст та місцезнаходження (шлях розташування) файлів;

- у разі потреби та наявності ресурсів здійснити побітове копіювання, створивши файлобраз носія;

- скопіювати файли з відеограмою та скриншотами зображення екрана монітора;

- вивести на екран монітора інформацію про контрольну суму кожного файла;

- приєднати та відформатувати другий носій, після цього скопіювати на нього всю інформацію з контрольного носія;

- інформацію про здійснений огляд внести до протоколу та роздрукувати його, після чого файли зберегти на контрольному і робочому примірниках носіїв разом з каталогом із доказовою інформацією;

- від'єднати носії з доказовою інформацією та упакувати. До вказаного алгоритму дій можна додати додаткові пункти за умови огляду віддаленого ресурсу комп'ютерної мережі щодо встановлення IP-адресисайта (ping), шляху проходження пакетів при обміні інформацією з ним, скопіювати їх на носій, призначений для запису та зберігання доказової інформації [154, с. 38].

Хотілось би також зазначити, що сьогодні значна кількість інформації зберігається у «хмарних сховищах», тобто розміщена поза місцезнаходженням фізичної чи юридичної особи. Тому присутні під час обшуку особи можуть використати наявні в них різноманітні гаджети, у тому числі мобільні телефони, для вчинення будь-яких дій з метою пошкодження, знищення, перетворення інформації, яка фактично може перебувати на відстані (навіть у межах приміщення, де відбувається обшук, тощо). З огляду на це, із тактичних міркувань, доцільно усім присутнім при обшуку особам, на початку обшуку повідомити про заборону використання під час проведення обшуку мобільних телефонів чи інших електронних пристроїв, які знаходять у них, та покласти їх на місце, доступне для поля зору слідчого, оперативного працівника, понятих, для здійснення контролю за невикористанням зазначених речей під час проведення обшуку [25, с. 19].

В розрізі цього слід зауважити, що кримінальним процесуальним законодавством не всі об'єкти дозволено вилучати. А на деякі об'єкти для

можливості їх вилучення існує специфіка. Тому, при визначенні статусу об’єктів, слід бути уважними.

Зокрема, як вбачається зі змісту п. 7 ч. 1 ст. 162 КПК України, до охоронюваної законом таємниці, яка міститься в речах і документах, належить й інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв`язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.Відповідно до ч. 6 ст. 163 КПК України слідчий суддя постановляє ухвалу про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, якщо сторона кримінального провадження доведе можливість використання як доказів відомостей, що містяться в цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів [164].

З цього приводу можна навести приклад. Так, прокурор вказав, що з метою всебічного, повного і неупередженого дослідження обставин кримінального правопорушення, необхідно отримати дозвіл на тимчасовий доступ до речей і документів, які перебувають у володінні операторів телекомунікаційних послуг (інтернет-провайдерів), а також вилучити їх копії, а саме документів, на підставі яких надаються (були надані) телекомунікаційні послуги користувачам установлених у ході досудового розслідування IP-адрес (договорів, угод, актів підключення, актів виконаних робіт та інших), які містять інформацію про абонентів (споживачів), місць (адрес) фактичного підключення, MAC-адрес, контактних даних споживачів (телефони, електронна пошта та інші). Як результат, слідчий суддя Печерського районного суду м. Києва надав дозвіл прокурору відділу Генеральної прокуратури України про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, з можливістю вилучення їх засвідчених належним чином копій у операторів телекомунікаційних послуг (інтернет-провайдерів), а саме у:ТОВ «Т.Е.С.Т.» -документів, на підставі яких надаються телекомунікаційні послуги

користувачам IP-адреси: 109.237.84.222, в тому числі документів (договорів, угод, актів підключення, актів виконаних робіт та інших), які містять інформацію про абонентів (споживачів), місць (адрес) фактичного підключення, MAC-адрес, контактних даних споживачів (номерів телефонів, електронну пошту тощо) за вказаною IP-адресою;ПАТ «УКРТЕЛЕКОМ» - документів, на підставі яких надаються телекомунікаційні послуги користувачам IP-адрес: 178.94.112.66, 37.52.240.234, 95.135.220.222, 46.201.91.86, в тому числі документів (договорів, угод, актів підключення, актів виконаних робіт та інших), які містять інформацію про абонентів (споживачів), місць (адрес) фактичного підключення, MAC-адрес, контактних даних споживачів (номерів телефонів, електронну пошту тощо) за вказаними IP-адресами;-ТОВ «УКРНЕТ» - документів, на підставі яких надаються телекомунікаційні послуги користувачам IP-адреси: 212.42.77.152, в тому числі документів (договорів, угод, актів підключення, актів виконаних робіт та інших), які містять інформацію про абонентів (споживачів), місць (адрес) фактичного підключення, MAC-адрес, контактних даних споживачів (номерів телефонів, електронну пошту тощо) за вказаною IP-адресою тощо[164].

Забороняється й тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв’язку, крім випадків, коли: їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, такі об’єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення; доступ до них обмежується їх власником, володільцем або утримувачем чи пов’язаний з подоланням системи логічного захисту. Для опечатування носіїв необхідно упакувати їх у жорстку негнучку коробку та опечатати її. Далі слід зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їх кількість). Коробка з носіями і опис поміщаються в поліетиленовий пакет, де горловина пакета міцно обв’язується шовковою (капроновою) ниткою і фіксується двома

подвійними простими вузлами, які розміщують на діаметрально протилежних сторонах [154, с. 39].

Слід зазначити, що обов'язковим є складання реєстру вилучених документів. Для надання документам юридичної сили та доказовості вони повинні мати такі обов'язкові реквізити: назва документа (форма, дата і місце складання; назва підприємства, від імені якого складено конкретний документ; зміст та обсяг цивільно-правової операції; посади осіб, відповідальних за здійснення цивільно-правової операції і правильність оформлення; особистий підпис або інші дані, що дають змогу ідентифікувати особу яка брала участь у здійсненні цивільно-правової операції. У разі необхідності підприємство може включити в документ додаткові реквізити, що потребує додаткових умов їх використання та збереження. Такими реквізитами можуть бути: ідентифікаційний код підприємства, номер документа, підстави для здійснення операції, наявність певних знаків, полос та ін. Також документи, які потребують наявність обов'язкового підпису, можуть бути підписані від руки, за допомогою кліше (факсиміле), символу або будь-яким іншим механічним способом, але при цьому документ повинен містити вказівку на особу, яка здійснила цивільно-правову операцію, з метою подальшої ідентифікації такої особи [35, с. 6]. У випадку, якщо шахрайство в інтернет-комерції вчинялося з боку шахраїв-підприємців, важливим напрямом під час проведення обшуку є ретельна перевірка записів, які ведуться в організації: документації у комп'ютерній системі; вихідна та оперативна інформація про діяльність підприємства; особисті дані про співробітників; список структур, з якими організація співпрацювала чи співпрацює тощо [111, с. 176]. Таку інформацію можна отримати від самого підозрюваного, або від інших осіб, які володіють будь-якими даними. В окремих випадках бажано, щоб підозрюваний був присутній при огляді його комп'ютера, оскільки саме він може надати найважливішу інформацію про особливості функціонування комп'ютерної системи: 1) паролі, коди доступу; 2) перелік інстальованих комп'ютерних програм (програм, які є у

комп'ютері); 3) місцезнаходження окремої інформації на машинному носії (окремих директорій, у тому числі прихованих) [16, с. 66; 126].

Ефективність такої рекомендації можна продемонструвати на наступному прикладі. Так, гр.-ка Д. за місцем свого фактичного проживання самостійно зареєструвалась в соціальній мережі «Instagram», де створила обліковий запис та, реалізуючи свій злочинний умисел, направлений на шахрайство, за допомогою комп`ютерної техніки, мобільного терміналу та підключення до Інтернет провайдеру «SkyLink» у всесвітній мережі Інтернет, на вказаному сайті розмістила оголошення з приводу продажу жіночого одягу. Однак, отримавши на свою картку гроші від потерпілоїгр.-ки. Т., товар останній так і не надіслала. Завдяки тому, що під час тимчасового доступу до речей та документів гр.-ка Г. надаладоступ до своїх акантів, обшук мав успішний результат [166].

Ще однією важливою слідчою (розшуковою) дією, що спрямована на одержання інформації з матеріальних джерел, є допит, який проводиться у 100 % випадків.

Процесуальні питання проведення допиту відображені у низці норм Кримінального процесуального кодексу України (далі – КПК). Так, у ст. 224 КПК окреслюється загальний процесуальний порядок проведення допиту, статтею 225 КПК визначені правові підстави та порядок допиту свідка, потерпілого під час досудового розслідування в судовому засіданні. Особливості допиту певної категорії осіб (малолітніх, неповнолітніх) висвітлені у ст. 226, 227, 490, 491 КПК тощо. Проведення допиту у режимі відео конференції при трансляції з іншого приміщення (дистанційне досудове розслідування) регламентується нормою ст. 232 КПК України [94; 4].

Разом з тим, на сьогоднішні існує низка проблем як процесуального, так і організаційно-тактичного характеру стосовно допиту. На перший погляд, проведення допиту не становить особливих труднощів. Між тим, варто погодитися із твердженням про те, що ця легкість лише удавана. Адже

допитувані далеко не завжди дають правдиві, повні й об’єктивні свідчення, тому досягти бажаного результату вдається після тривалого процесу спілкування з допитуваним, використовуючи при цьому певний комплекс тактичних прийомів [94; 4].

Запорукою успіху у будь-яких провадженнях, у тому числі й щодо шахрайства в інтернет-комерції, є підготовка до допиту.

Як показав аналіз судово-слідчої практики та опитування респондентів, окрім загальновизнаних елементів підготовки (вивчення матеріалів провадження, вивчення особи допитуваного, обрання місця, часу проведення допиту, підготовка техніко-криміналістичних засобів для фіксування результатів допиту тощо), слідчий повинен опрацювати й законодавство, що регулює правовідносини в режимі он-лайн з 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 установлення автентичності в онлайн режимі тощо.

До того ж, слід погодитися із К. О. Чаплинським, який зазначає, що допитувані не завжди зацікавлені у повному й всебічному розкритті та розслідуванні злочину, що не може не впливати на правдивість їх показань. Окрім того, на потерпілих і свідків здійснюється негативний вплив з боку злочинців, що нерідко тягне до зміни їхніх показань. Зважаючи на це, успішне проведення допиту і отримання позитивних його результатів залежить від якості володіння слідчими знаннями про закони мислення, логічні методи і прийоми, закономірності психології та тактичні прийоми, що розроблені у криміналістиці [197, с. 198].Тому слідчому доцільно опрацювати ці питання, щоб під час безпосереднього допиту апелювати отриманими

знаннями та застосовувати практичні навички щодо психологічного і тактичного впливу на допитуваного.

Враховуючи отриману інформацію, слідчий повинен тактично правильно визначити послідовність допитів, особливо, якщо злочини вчинялися у складі групи. Для цього слід максимально бути поінформованим відносно вікових, морально-психологічних характеристик, ролі та характеру участі кожного з учасників, враховувати їх зацікавленість у кінцевому результаті по справі. Як показує практика, більш ефективним є отримання в першу чергу показань від особи, яка, на думку слідчого, мала другорядну роль у вчиненні злочину та вчинила злочин вперше. Більш схильні до надання показань також особи, у відношенні яких є велика кількість доказів. З метою тактичного впливу на учасника допиту, необхідно підготувати докази, які почергово пред'являтимуться під час допиту. Найбільш часто з цією метою використовуються висновки експертиз та різноманітні документи, в яких відображається доказова інформація або документи, що були засобом вчинення злочину, а також інші предмети, що можуть бути речовими доказами [125].

З метою виявлення певних протиріч у показаннях та використання їх під час подальшого допиту, слідчий повинен заздалегідь проаналізувати показанняінших осіб, результати проведення інших слідчих (розшукових) дій, які містять докази щодо розслідуваної події. При цьому доцільно вивчити додаткову інформацію, що допоможе деталізувати, уточнити показання допитуваного, виявити невідповідність певних фактів [128, с. 118-119].

Важливою складовою допиту є його предмет, тобто перелік обставин, що підлягають встановленню. При цьому, залежно від процесуального статусу особи, яка допитується, предмет допиту може різниться.

Як показав аналіз судово-слідчої практики та опитування респондентів, у провадженнях щодо шахрайств в інтернет-комерції, обставинами,що підлягають встановленню, під час допиту потерпілого, є:

- за допомогою яких засобів дистанційного зв'язку потерпілий дізнався про товар або послугу (телекомунікаційні мережі, телебачення, Інтернет тощо;

- чи було приділено увагу вивченню репутації продавця;

- чи було накладено електронний підпис для закріплення угоди. При цьому, слід пам’ятати, щоспеціальне правове регулювання передбачено для електронного підпису, який повинен відповідати таким критеріям: унікальним чином бути пов’язаним із підписувачем; бути здатним його ідентифікувати; створюватися на підставі засобів, що перебувають під особистим контролем підписувача; бути пов’язаним з даними, яких він стосується, так, щоб будь-яка подальша зміна даних могла бути виявлена [52, с. 90];

- що саме рекламувалося, основні характеристики продукції, чи були фотознімки товару;

- які були умови продажу (оплата, доставка тощо);

- яким чином відбувався зв'язок із метою обговорення предмету договору (відеозвязок, телефонний дзвінок, смс спілкування тощо);

- чи запам’ятав потерпілий зовнішність особи, яка виявилася шахраєм (у разі застосування відеозв’язку);

- чи робив потерпілий скріни екрану монітора (інтернет-магазину), спілкування із шахраєм тощо;

- яким чином відбувалася автентифікація та авторизація користувача;

- що було підтвердженням вчинення електронного правочину (чи були вказані умови та порядок обміну (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 тощо;

- 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 із продажу товарів (послуг) в онлайн режимі не виконані;

- чи висувалися потерпілим претензії і як реагували на ці претензії шахраї;

- чи було прохання відправки товарів накладним платежем;

- скільки пройшло часу з моменту вчинення шахрайства до звернення громадян до органів Національної поліції чи направленнязвернення на електронну скриньку Сервісної служби кіберполіції тощо.

Під час проведення допиту підозрюваного слід ставити питання, що стосуються таких обставин: виникнення злочинного задуму; відомості про об'єкт посягання, мотив злочину, ставлення особи до злочинних наслідків; способи підготовки та вчинення злочинів, послідовність злочинних дій, а також особливості приховування злочинної діяльності (її характер); час, місце, обстановка та механізм учинення злочинів; відомості про особу злочинця; умови, за яких допитуваний спостерігав будь-які предмети або явища; психологічний і фізичний стан особи в момент сприйняття чи після нього; загальна здібність допитуваного до певного сприйняття, запам'ятовування та відтворення; обставини, що сприяли або перешкоджали учиненню злочинів; способи формування організованої групи та характер злочинної діяльності; виявлення психологічної та функціональної структури групи (якісний склад, рівень організованості) та розподілу функціональних обов'язків; кількісний склад групи при учиненні кожного епізоду злочинної діяльності, конкретні дії кожного, навички володіння зброєю та прийомами боротьби; виявлення осіб, які не брали безпосередньої участі у вчинених злочинах, але обізнані про їх підготовку, вчинення або приховання; наявність корумпованих зв'язків і зв'язків з іншими злочинними групами; способи протидії розслідуванню та впливу на потерпілих, свідків і членів групи, які дають правдиві показання; наявність у групі конфліктів, протиріч і

розбіжностей; способи легалізації отриманих прибутків і відтворення злочинної діяльності; встановлення осіб, які залишилися на волі та продовжують злочинну діяльність або налагоджують зв'язки між членами групи та намагаються створити єдину, вигідну для усіх лінію поведінки та ін. [196, с. 210].

При допиті підозрюваної особи слідчому необхідно переконати зазначеного суб'єкта у сприянні слідству. До того ж, допити підозрюваних у кримінальних провадженнях за фактами вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет спрямовувалися на: з'ясування події кримінального правопорушення, обставин повідомлення, характер дій кожного співучасника – у 100 %; з'ясування причин та умов, що сприяли вчиненню шахрайства – 39 %, з'ясування даних що мають тактичне значення – 34 %; виявлення співучасників шахрайських дій – 29 % [205, с. 160].

При цьому, слід мати на увазі, що тактика безпосереднього допиту підозрюваного істотно різниться, тобто, якщо потерпілий чи свідок здебільшого ідуть на контакт і схильні до спілкування, то у відношенні підозрюваних слід використовувати великий арсенал тактичних прийомів, серед яких: пред'явлення доказів;оголошення показань інших осіб; використання суперечностей у показаннях однієї й тієї ж особи;створення враження поінформованості слідчого; фактор раптовості тощо[125].

Як зазначає К.О. Чаплинський, слідчий повідомляє підозрюваному про докази та інші матеріали, які викривають злочинців або спростовують їх показання, і демонструє їх у певній послідовності, визначаючи надалі позицію допитуваних як на допиті, так і під час усього розслідування [197, с. 244–245].

З цього приводу Є. В. Дехтярьов наголошує, що типовою особливістю шахраїв є наявність досконалих комунікативних якостей: вміння наладжувати контакт, розташовувати до себе. Більшість із них мають здібність до певної манери поведінки зі співбесідниками різних за складом характеру, щоб, за

необхідності, обрати такий спосіб взаємовідносин, який є найбільш вигідним для відстоювання своєї позиції в ході проведення слідчих дій. Зазначене вимагає від слідчого прояву рішучості у встановленні тих або інших обставин справи, критично ставитися до поведінки допитуваного та змісту його показань. Цілком логічно, що за цих умов важливу роль у подоланні протидії допитуваного відіграє таке оперування доказами, яке дозволяє викликати в підозрюваного впевненість у тому, що слідство має в своєму розпорядженні певні та беззаперечні фактичні дані про його причетність до обманного заволодіння майном. Головною ж рисою застосування тактичних прийомів під час допиту підозрюваних у вчиненні шахрайства є використання методу пред'явлення доказів за наростаючою. Саме в цьому разі створюється сприятлива обстановка, коли неправдиві свідчення підозрюваного спростовуються новим пред'явленим доказом. Такий порядок реалізації наявного в слідчого доказового матеріалу грунтується на тому, що не рекомендується пред'являти його весь одразу, адже не виключається можливість того, що з урахуванням обізнаності, підозрюваний може висунути не тільки правдоподібну, але й складно спростовну версію. Варто зауважити, що достатньо ефективно під час допитів зазначеної категорії осіб зарекомендував себе такий тактичний прийом, як «мислення вголос». Його сутність полягає б тому, що перед підозрюваним розгортаються варіанти його поведінки з урахуванням повідомлення ним неправдивих відомостей, з переліченням шляхів та засобів спростування цих показань та викриття неправди [42, с. 290-291].

Предметом допиту підозрюваного у провадженнях щодо шахрайства в інтернет-комерції є встановлення наступних обставин:

- дані про особу підозрюваного (стать, вік, сімейний стан, освіта, судимість, наявність хронічних захворювань, образ життя);

- коло інтересів допитуваного, його відношення до сфери торгівлі;

- через які соціальні мережі вчинялися шахрайські дії;

- чи офіційно діяв сайт, де розміщувалася інформація про продаж товарів та послуг;

- чи знайомий він із потерпілим і які має з ним стосунки;

- які конкретно дії, пов'язані з інтернет-комерцією, було ним здійснено (створення сторінки в соцмережі; створення вебсайту; отримання доступу до сайту іншої особи);

- наявність умислу, коли він виник і скільки осіб було обмануто;

- коло спілкування допитуваного, факти, що свідчать про наявність співучасників;

- чи допомагав підозрюваному хтось у здійсненні злочинного умислу, які були у цієї особи функції (технічна допомога, спілкування з потерпілими, постачання товарів тощо) тощо.

Серед кола осіб, що підлягають допиту як свідки у досліджуваній категорії проваджень, можна назвати:

- працівники, що супроводжують комерційні угоди в онлайн режимі;

- представники та працівники юридичної особи, яка використовувалася під час вчинення злочину тим чи іншим способом;

- спеціалісти, що мають професійний досвід у галузі інформатики та комп'ютерної техніки, програмування, в тому числі особи, які приймали участь у якості спеціалістів підчас слідчих (розшукових) дій. Свідки часто володіють спеціальною, професійною освітою (у сфері КТ, банківського електронного обігу коштів) або в цілому є обізнаними у питаннях використання інформаційних технологій та ІТ-технологіях [154, с. 40];

- особи, які знаходилися у приміщенніінтернет-кафе, банку;

- банківські працівники;

- родичі та знайомі потерпілого;

- родичі та знайомі підозрюваних тощо.

Слід погодитися із К. В. Аріт, який зазначає, що значущість повідомлюваних свідками відомостей залежить від низки чинників, серед яких переважає бажання, продиктоване обов'язками громадянина припинити

злочинну діяльність певних осіб. Саме ця обставина зумовлює важливість визначення груп свідків, їхньої спрямованості, потенційних можливостей для одержання даних, що сприяють розслідуванню злочинів. Повідомлювана свідками інформація в загальному вигляді залежить від ступенів поінформованості останніх, однак, у більш докладній градації й від інших характеристик [6, с. 107].

Для усунення розбіжностей у показаннях потерпілих, свідків, підозрюваних та інших учасників кримінального процесу у досліджуваній категорії справ у 95 % випадків проводиться одночасний допит двох або більше осіб.

Істотну роль у встановленні ступеня провини кожного з співучасників у кожному епізоді та усунення протиріч має проведення одночасних допитів. Згідно ст. 224 КПК України, одночасні допити можуть проводитися між двома чи більше вже допитаними особами. З цього виходить, що законодавець не лімітував кількість осіб, які є учасниками такого виду допиту. Втім, із тактичних міркувань вважаємо правильним звести максимальну кількість одночасно допитуваних осіб до трьох. Якщо учасниками такого допиту буде більша кількість осіб, слідчому буде складно зосередити увагу на поведінці, міміці, реакції кожного з допитуваних. А для виявлення протиріч серед членів ОЗГ це дуже важливо. Доцільно починати показань учасника, який, на погляд слідчого, надає найбільш правдиві показання або учасника, який мав опосередковану роль у вчиненні злочинів [198].

Результати дослідження показали, що у 89 % випадків вказана СРД проводилася між підозрюваним і потерпілим, у 8 % – між підозрюваними особами, у 4 % – між підозрюваним і свідками. Достатньо низький відсоток проведених одночасних допитів за участю свідків визначається наступними обставинами. Як показало проведене анкетування, даний факт можна пояснити неврегульованістю механізму притягнення до відповідальності осіб, які надають завідомо неправдиві показання та відмовляються їх надавати

взагалі [205, с. 162].

Така слідча (розшукова) дія, як пред'явлення для впізнання, у кримінальних провадженнях щодо шахрайства в інтернет-комерції проводиться рідко (8 %), адже спілкування між шахраєм та потерпілим в основному 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 об'єктами пред'явлення для впізнання обрати або живих осіб, або осіб, зображених на фотокартках.

Може постати питання й про пред'явлення для впізнання особи за матеріалами відеозапису.

Натомість, КПК України лише визначає, що матеріали відеозапису зі зображенням особи, яка підлягає впізнанню, можуть бути пред'явлені лише за умови зображення на них не менше чотирьох осіб, які повинні бути тієї ж статі і не повинні мати різких відмінностей у віці, зовнішності та одязі з особою, яка підлягає впізнанню [161, с. 101]. А це, як свідчить практика, дуже складно.

Якщо спілкування здійснювалося через телекомунікаційні пристрої, цілком вірогідним є пред'явлення для впізнання за голосом, щоповинно здійснювалися таким чином, щоб візуальний контакт між впізнаючим та особами, які пред'явлені для впізнання, був відсутній, аби виключити вірогідність вибору за будь-якою іншою ознакою; зміст розмови, який буде сприймати впізнаючий, має містити відомі для нього слова або словосполучення, які він вже чув від особи, образ якої зберігся в його пам'яті [89, с. 392].

На всіх історичних етапах розвитку суспільства людьми застосовувалися різні засоби отримання інформації для пошуку злочинця. Не виключенням є й негласні слідчі (розшукові) дії. Законодавець вказує на

спрямованість НСРД, зазначаючи, що вони проводяться з метою отримання або перевірки доказів, якщо відомості про злочин або особу, що його вчинила неможливо отримати в інший спосіб (ч. 2 ст. 246 КПК) [77, с. 23]. Основним функціональним призначенням негласних слідчих (розшукових) дій в оновленій системі кримінального процесу України є забезпечення оптимальних шляхів використання у кримінально-процесуальному провадженні інформації, здобутої із використанням негласних сил і засобів [39, с. 173].

Як показав аналіз судово-слідчої практики, у провадженнях щодо шахрайства в інтернет-комерції найчастіше проводяться такі негласні слідчі (розшукові) дії: зняття інформації з транспортних телекомунікаційних мереж (84 %); зняття інформації з електронних інформаційних систем (79 %); установлення місцезнаходження радіоелектронного засобу (91 %) тощо. Поширеність саме таких НСРД пов’язана з тим, що спілкування між шахраєм та потерпілим, особливо під час підготовки до вчинення шахрайських дій в інтернет-комерції, здебільшого відбувається через транспортні телекомунікаційні мережі та через мережу Інтернет (смс повідомлення, відеозв’язок, листування через електронну адресу).

Зміст розмов у ході використання певного виду зв’язку, а також дані електронної переписки можуть містити достатньо багато інформації щодо обставин справи тощо [198].

Вказане викликає необхідність вдосконалення тактики та методики отримання інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем. У зв’язку із цим, основним напрямом розслідування шахрайства, за умов використання сучасної техніки, є:

- по-перше, встановлення механізму слідоутворення в засобах апаратно-програмного забезпечення систем мобільного зв’язку;

- по-друге, встановлення механізму слідоутворення в засобах комп’ютерної техніки тощо;

- по-третє, отримання та вибірка відомостей про надані телекомунікаційні послуги та взаємоз'єднання телекомунікаційних мереж;

- по-четверте, отримання та вибірка відомостей про здійснення дій, пов'язаних із втручанням у роботу електронно-обчислювальної техніки [126].

У ході проведення зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України) негласно здійснюється фіксація телефонних розмов, іншої інформації та сигналів, зокрема служби коротких повідомлень (коротких текстових повідомлень в телекомунікаційних мережах, SMS, ShortMessageService), послуги мультимедійних повідомлень (зображення, звук тощо, MultimediaMessagingService, MMS), факсимільного зв'язку, модемного зв'язку, зв'язку «банкклієнт» тощо) [99, с. 119]. Для одержання таких відомостей необхідні складні програмно-технічні комплекси обладнання, які дозволяють одержувати доступ та здійснювати моніторинг повідомлень, які передаються між абонентами комунікаційної мережі [137, с. 141].

У цьому розрізі О. І. Хараберюшдії суб'єктів кримінального провадження щодо отримання інформації з телекомунікаційних мереж поділяє на:

1) зняття інформації з транспортних телекомунікаційних мереж (НСРД, передбачена ст. 263 КПК України), яке в свою чергу поділяється на:

- конспіративне перехоплення, контроль телефонних розмов та фіксацію їх змісту з використанням технічних засобів негласного отримання інформації;

- перехоплення електронних сигналів та повідомлень з використанням технічних засобів негласного отримання інформації.

2) установлення місцезнаходження радіоелектронного засобу шляхом:

- пеленгування місцезнаходження кінцевого обладнання мереж телекомунікацій оперативно-технічними підрозділами при виконанні доручень у порядку ст. 40 КПК України – як НСРД «установлення

місцезнаходження радіоелектронного засобу», передбачена ст. 268 КПК України;

- затребування компетентними органами розслідування інформації про взаємоз'єднання телекомунікаційних мереж з метою отримання та вибірки відомостей про надані телекомунікаційні послуги – як процесуальна дія, передбачена ст. 93 КПК України [191].

З приводу установлення місцезнаходження радіоелектронного засобу слід зазначити, що сьогодні сучасна теорія кримінального процесуального права характеризується наявністю двох точок зору з приводу віднесення останнього до НСРД. Відповідно до першої вчені не відносять установлення місцезнаходження радіоелектронного засобу до слідчих дій, обґрунтовуючи свою позицію відсутністю зазначеної НСРД у ч. 2 ст. 246 КПК України. Так, наприклад на думку таких дослідників, як В. Г. Гончаренко, В. Т. Нор, М. Є. Шумило, до НСРД належать ті слідчі дії, що передбачені ч. 2 ст. 246 КПК України. Натомість, слід погодитися із А. А. Ковалем, який вважає, що немає жодної підстави не вважати установлення місцезнаходження радіоелектронного засобу НСРД, оскільки остання характеризується тими самими ознаками, що й інші НСРД: 1) закріплення установлення місцезнаходження радіоелектронного засобу НСРД на законодавчому рівні; 2) підставою її проведення, як і інших НСРД, є ухвала слідчого судді; 3) вона спрямована на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні [77, с. 31].

Ця НСРД, відповідно до ст. 268 КПК України, полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, зокрема мобільного терміналу, систем зв'язку й інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо внаслідок його проведення можна встановити обставини, які мають значення для кримінального провадження. Фактично ж слідчий ініціює її проведення в кримінальних провадженнях різного ступеня тяжкості

задля визначення параметрів базових станцій операторів телекомунікацій, що забезпечують роботу в певному місці кінцевого обладнання систем зв'язку, і місцезнаходження інших радіовипромінювальних пристроїв, активованих у мережі операторів рухомого (мобільного) зв'язку [154, с. 41].

Технічні та програмні засоби операторів стільникового зв'язку дозволяють за номером IMEI телефонного апарату (смартфону) не тільки визначати номер SIM-карти, з яким цей апарат використовується в певний момент часу, та отримувати інформацію про абонента, зареєстрованого в мережі під цим номером, але і локалізувати місцезнаходження цього апарату з точністю до 50 метрів, якщо він знаходиться у ввімкненому стані [104, с 203].

Об'єктами зняття інформації з електронних інформаційних систем є: електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку, які накопичують, обробляють, зберігають або передають відомості, пов'язані із вчиненням тяжких та особливо тяжких злочинів, у тому числі до цих об'єктів належить електронна поштова скринька. Відомо, що електронна поштова скринька є одним із зручних, сучасних способів спілкування, з використанням якої для задоволення потреб учасників такого спілкування, інформація може передаватися за наявності для цього умов, у будь-яку частину світу [174, с. 117]. Водночас, зняття інформації з електронних інформаційних систем реалізується шляхом пошуку слідчим або інспектором кіберполіції (за дорученням слідчого) в різноманітних Інтернет-спільнотах відкритої інформації про особу злочинця. Виконавець за результатами дії складає протокол, у якому фіксує такі відомості: персоналізовані відомості про особу злочинця; ознака, за якою об'єднують коло осіб, що потрапляють під підозру; зв'язки особи, що потрапила під підозру; відомості, що можуть сприяти розв'язанню інших тактичних завдань (пошук свідків, потерпілих, забезпечення встановлення мотивів злочину тощо). До протоколу зняття інформації з електронних інформаційних систем або її частини додають

відповідні носії електронної інформації, що містять файли з відеограмою та зображенням екрана монітора (або знімками екрану, англ. screenshot), створеними під час дослідження системи, також їх роздруківки як додатків до протоколу [154, с. 41].

Отже, при розслідуванні шахрайства в інтернет-комерції проведення слідчих (розшукових) дій та НСРД надає змогу значно ефективніше здійснити комплекс заходів щодо документування злочинної діяльності, викриття винних та притягнення їх до відповідальності.

3.2. Криміналістична профілактика у провадженнях за фактами вчинення шахрайства в інтернет-комерції

Слідчий у процесі розслідування злочинів, поряд із встановленням і доказуванням обставин їх вчинення, повинен чітко усвідомлювати необхідність виконання іншої, не менш важливої функції – запобігання кримінальним правопорушенням у майбутньому. Цілком логічним, на наш погляд, є включення питань профілактичної діяльності слідчого в методику розслідування злочинів як окремого її структурного елемента [218, с. 58].

Натомість, слід зазначити, що дотепер тривають дискусії з приводу змістовної частин профілактичної діяльності у криміналістичному розумінні.

Деякі вчені включають у предмет криміналістичної профілактики:

- закономірності утворення, виявлення та дослідження слідів прояву криміногенних обставин під час підготовки, вчинення і приховання окремих видів і категорій злочинів відомими криміналістам способами (незалежно від того, чи застосовувались такі способи злочинцями, чи застосування їх є можливим і прогнозується криміналістами);

- техніко-криміналістичні засоби захисту об’єктів від злочинних посягань, що сприяють виявленню і припиненню злочинів, а також

використовуються з метою отримання, накопичення і видачі інформації про знаряддя і засоби, що використовуються під час вчинення злочинів, та осіб, схильних до їх вчинення;

- техніко-криміналістичні засоби, прийоми і методи виявлення, фіксації і дослідження криміногенних обставин;

- тактичні прийоми і засоби найбільш ефективного виявлення і усунення криміногенних обставин, а також запобігання і припинення злочинів;

- криміналістичні методи або системи прийомів виявлення і усунення причин і умов вчинення злочинів, а також припинення і попередження злочинів [183, с. 124].

Інші визначають криміналістичну профілактику, як діяльність уповноважених суб'єктів і напрям наукових досліджень, який базується на загальних кримінологічних рекомендаціях по встановленню причин і умов, що сприяють конкретним злочинам, вжиттю спеціальних криміналістичних заходів для їх профілактики, запобігання і припинення [106, с. 33].

Важливий внесок у розвиток поняття предмета криміналістичної профілактики зробив І. Я. Фрідман. Своє визначення предмета криміналістичної профілактики автор формулює так: «Криміналістичне вчення про профілактику вивчає закономірності виникнення обставин, що сприяють правопорушенням, їх виявлення, дослідження, оцінки і використання в попереджувальних цілях». Засоби і методи запобігання злочинам, на думку І. Я. Фрідмана, повинні розроблятися наукою криміналістикою і бути невід’ємною частиною її предмета і системи. На відміну від них, загальні питання криміналістичної профілактики слід розглядати самостійно, не в рамках наявних розділів, а як теоретичну частину криміналістичної профілактики, що утворить її окрему теорію. Він зауважував, що криміналістика повинна своїми спеціальними криміналістичними прийомами і методиками систематично і планомірно сприяти виявленню обставин, що сприяють вчиненню злочинів, розробці

заходів, спрямованих на їх усунення, готувати профілактичні рекомендації організаційного та технічного характеру (наприклад, розробляти спеціальні технічні пристрої), спрямовані на припинення конкретного злочину, попередження злочинів та інших правопорушень, аналогічних розслідуваному [183, с. 124; с. 95; 189].

Отже, як показав аналіз юридичної літератури, серед основних профілактичних заходів здебільшого вказуються виявлення причин та умов, що сприяють вчиненню злочинів, а також застосування заходів щодо їх усунення та припинення кримінальних правопорушень.

При цьому, як зазначає А. Ф. Волобуєв, успішне розв'язання проблеми встановлення причин та умов конкретного злочину можливе лише тоді, коли це завдання чітко усвідомлене, визначене з самого початку розслідування за кримінальним провадженням і планомірно вирішується паралельно з встановленням інших обставин [31, с. 345].

Проте, слід звернути увагу, що законодавець виключив взагалі у чинному кримінальному процесуальному кодексі норму, яка передбачала б заходи щодо усунення причин та умов, що сприяли вчиненню злочинів. На відміну від кримінально-процесуального кодексу 1961 р., де передбачався обов’язок органів дізнання, слідчого, прокурора при провадженні дізнання, досудового слідства і судового розгляду кримінальної справи виявляти причини та умови, що сприяли вчиненню злочину та вжити заходи по їх усуненню шляхом винесення відповідного подання (відповідно до ст. 23, 23[1] КПК), в ньому також чітко визначені суб’єктний склад та правові форми реагування уповноважених на те осіб (органу дізнання, слідчого, прокурора). Коментуючи цю законодавчу ініціативу, М. М. Єфімов зауважує, що в уповноважених осіб, які здійснюють досудове розслідування (слідчий, дізнавач, прокурор), повинні мати можливості хоча б зробити мінімум, щоб уникнути в подальшому вчинення подібних протиправних діянь [56, с. 342].

О. О. Черненко взагалі критично зауважує, що після набуття чинності нового КПК України у нормативному закріпленні профілактичних функцій

слідчих склалася суперечлива ситуація. З одного боку, положення нового кодексу не визначають обов'язки слідчих, пов'язані з виконанням загально-кримінологічної чи спеціальної профілактики. З іншого боку, в Законі України «Про поліцію» запобігання злочинам та іншим правопорушенням було віднесено до основних обов'язків правоохоронців, які традиційно поширювалися на усі підрозділи та служби МВС України, в тому числі – на підрозділи Головного слідчого управління [199, с. 185].

Більшість авторів взагалі виступають щодо внесення до чинного КПК України доповнення про внесення подання на розгляд державних органів та посадових осіб [8, с. 86]. Натомість, В. М. Плетенець критично зауважує, що, запровадження лише даної норми в чинний КПК України, без зміни ставлення уповноважених суб'єктів до розглядуваного процесуального засобу впливу, ситуацію не змінить. Тому, превентивній діяльності має бути приділено належну увагу з боку дослідників та практиків, що б вивести її на якісно новий рівень. Тільки тоді можна говорити про вплив розглядуваної діяльності правоохоронних органів на злочинність як явище. Особливого значення ця діяльність набуватиме в умовах можливості реалізації протидії, усунення яких розглядатиметься запорукою успіху їх подолання. Для усунення причин та умов вчинення кримінального правопорушення, що були виявлені в ході розслідування, уповноважена особа може направити подання до відповідного органу чи структури, незалежно від форм власності. Проте, усунення виявлених уповноваженими особами причин та умов протидії досудовому розслідуванню, переважно, покладається на них самих. Саме від якості реалізації суб'єктами розслідування застосованих засобів та заходів визначається ступінь інтенсивності протидії та можливості її подолання. Таким чином, усвідомлення того, що реалізовувати заходи доведеться самому, а не доручати комусь, сприятиме підвищенню ефективності здійснення діяльності з недопущення або зведення до мінімуму можливості формування умов протидії досудовому розслідуванню [135, с. 337].

Тому, як на нашу думку, необхідно повернути закріплення в КПК України обов'язку виявляти органам досудового розслідування причини й умови, що сприяли вчиненню кримінальних правопорушень, а також вносити до відповідного державного органу, громадської організації або посадової особи подання стосовно вжиття заходів для усунення вищезазначених умов і причин.

Водночас, як справедливо зауважує В. Г. Дрозд, удосконалення кримінального процесуального законодавства України повинно відбуватися тільки з урахуванням загальновизнаних європейських стандартів і принципів здійснення кримінального судочинства [46, с. 59], а також відповідати сучасним реаліям.

У юридичній літературі стосовно боротьби та розслідування шахрайства можна побачити неодноразові спроби описати причини, чому таке явище набуло масового явища.

Слід відзначити позитивним науковий підхід А. Ф. Волобуєва, який, досліджуючи злочини у сфері підприємництва, у тому числі й комерційні (торгівельні) шахрайства, розподілив причини та умови їх вчинення на суб'єктивні і об'єктивні. До суб'єктивних умов вчений відніс наступні фактори:віра певної частини населення в те, що в умовах ринкових відносин можна збагатитися швидко і, головне, не прикладаючи великих зусиль. Саме цю умову використовують підприємці-шахраї;довірливість людей до реклами, особливо коли вона проводиться з широким використанням різноманітних засобів на значній території (преси, телебачення, рекламних написів на спеціальних щитах і будівлях). Уява людей про можливість швидкого збагачення формувалася і під суттєвим впливом недобросовісної (а точніше, шахрайської) реклами на початку 90-х рр. комерційними структурами типу АТ «МММ», «Український будинок Селенгу» та іншими. Ґрунтується така віра на глибокому психологічному усвідомленні, що ЗМІ контролюються державою і все що повідомляється ними сприймається як офіційна позиція;схильність деяких підприємців у гонитві за високим прибутком до

занадто ризикованих комерційних операцій. Ця риса проявляється при укладанні сумнівних угод щодо закупівлі великих партій дефіцитного товару на умовах 100% попередньої оплати, наданні кредиту без належної перевірки можливостей партнера та інших. Прагнення одержання високих прибутків, випередження конкурентів при укладанні вигідних договорів активно експлуатують підприємці-шахраї, вдаючись головним чином до фальсифікації різноманітних документів для введення в оману необережних бізнесменів;недостатньо ретельна перевірка кандидатур при найманні на роботу, пов'язану з великими матеріальними цінностями, грошима, виконанням особливо важливих функцій. В комерційних структурах не завжди приділяється належна увага підбору кадрів, робота яких має відношення до операцій з коштами. В результаті на посади менеджерів, бухгалтерів, економістів, спеціалістів в галузі комп'ютерної техніки потрапляють особи з кримінальною спрямованістю, які використовують своє службове становище для особистого збагачення за рахунок компанії, в якій вони працюють;недоліки в організації служби економічної безпеки підприємств і банків. Звичайно дозволити собі службу економічної безпеки може тільки достатньо велике підприємство;недоліки в діяльності контролюючих і правоохоронних органів, які своєчасно не виявляють або не реагують на правопорушення в підприємницькій діяльності;корумпованість державного апарату управління. Це одна з найбільш криміногенних умов економічної злочинності, яка є зараз надзвичайно складною і болючою проблемою в Україні [31, с. 351-353].

До об'єктивних умов можуть бути віднесені наступні фактори, які безпосередньо не залежать від свідомості і волі населення:

- повільність і суперечливість соціально-економічних реформ на шляху переходу до ринкової економіки, відсутність чіткої концепції (програми) таких реформ;

- загальноекономічна і фінансова криза, яка продовжує поглиблюватися (тягне за собою зростання безробіття, технологічний занепад виробництва, неплатоспроможність підприємств);

- масове зубожіння населення (більшість його знаходиться на межі і за межею бідності);

- недосконаліть законодавства, що регулює фінансово - господарські відносини (часті зміни в законодавстві, непомірний податковий тиск на підприємця);

- відсутність ефективної системи державного контролю за діяльністю комерційних структур;

- наявність тіньової економіки співвідносної за своїми матеріальними і фінансовими ресурсами з економікою легальною (є живильним середовищем для організованої злочинності).

Приведені суб'єктивні і об'єктивні фактори переплітаються між собою і впливають один на одний, створюючи сприятливі умови для економічної злочинності, зокрема для її організованих форм [31, с. 354-355].

Разом з тим, матеріали судово-слідчої практики, анкетування працівників поліції та аналіз юридичної літератури, дозволили виділити такі причини та умови, що сприяють вчиненню комерційних інтернет-шахрайств:

Об'єктивні причини та умови:

- наявність законодавчих колізій щодо здійснення комерційних інтернет-угод. Так, згідно з роз'ясненням Міністерства економічного розвитку і торгівлі України у листі № 3502-05/43517-14 від 19.11.2012 р. суб'єкти господарювання, які здійснюють торгівлю за допомогою мережі Інтернет, повинні керуватися вимогами Правил продажу товарів на замовлення та поза торговельними або офісними приміщеннями. Між тим, не дивлячись на існування цих Правил, законодавчо вимоги щодо порядку створення таких магазинів не достатньо визначені, що не заважає шахраям створювати інтернет-магазини, а потім їх ліквідовувати. Це створює

підґрунтя для існування магазинів у мережі Інтернет, що діють за принципом фірм-одноденок [140; 205](78 %);

- недостатня нормативна урегульованість питань пов'язаних із створенням, введенням/виведенням коштів, ліквідацією електронних гаманців, що полегшує використання їх у злочинній діяльності. Основні властивості віртуальних гаманців, якими зловживають злочинці, полягають у можливості: швидкого, дешевого проведення трансакцій і легкості обходу обмежень, зокрема за сумами платежів; організації та проведення нелегальної діяльності за допомогою мережі Інтернет, доходи від якої надходять за допомогою платежів в електронних грошах; ухилення від сплати податків; приховування слідів трансакції (послідовного ряду трансакцій); використання третіх осіб; де-персоніфікованого введення/виведення готівки; «обходу» банківської системи, яку жорстко регулюють з питань легалізації коштів, отриманих злочинним шляхом [32, с. 275] (71 %);

- зростання випадків переведення грошей через платіжні системи WebMoney, PayPaЬ, QIWI, МспеуЬоокегв, які позбавляють можливості ідентифікувати особу, яка знімає кошти з рахунку [66, с. 75] (35 %);

- зростання випадків оплати товарів та послуг криптовалютою, статус якої дотепер не визначений (8 %);

- недостатня сформованість єдиного понятійного апарату щодо середовища, в якому вчиняються кримінальні правопорушення, пов'язані із використанням комп'ютерних технологій (31 %);

- низький рівень розкриття кримінальних правопорушень, пов'язаних із купівлею-продажем товарів через мережу Інтернет, в той час, як латентність є дуже високою (37 %);

- складність доведення факту вчинення обману в мережі Інтернет, що породжує нові випадку з боку одних і тих самих осіб (35 %);

– розповсюдженість недостовірних пропозицій у ЗМІ та мережі Internet (79 %);

- зниження рівня життя населення, що змушує шукати пропозиції в

Інтернеті за більш вигідними цінами, аніж у торгівельних центрах (82 %);

- недостатній контроль з боку суб'єктів, які повинні здійснювати функції з контролю за діяльністю суб'єктів підприємницької діяльності сфери (81 %);

- неоднозначність судової практики щодо шахрайств у мережі Інтернет (67 %) тощо.

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

- надання громадянами переваги укладанню дистанційного варіанта угод щодо купівлі-продажу товарів та послуг, що виключає прямий фізичний контакт продавця та покупця (81 %);

- халатне відношення до перевірки репутації підприємця, який пропонує об'єкти комерційного призначення і Інтернеті та покупця, який такі об'єкти (послуги) бажає отримати (81 %);

- халатне відношення до вивчення інформації, що міститься в електронній формі щодо умов купівлі-продажу товарів та послуг (81 %);

- халатне відношення до вивчення змісту документів, в яких зафіксовано укладання дистанційної угоди (69 %);

- надто велика довірливість, безпечність та необачність громадян (91%);

- професійно-моральна деформація суб'єктів підприємницької діяльності, та схильність їх до обману з метою наживи (81 %);

Слід зауважити, що криміналістика повинна систематично і планомірно сприяти не тільки виявленню обставин та причин, що сприяють вчиненню злочинів, а й сприяти розробці заходів, спрямованих на їх усунення, а також готувати профілактичні рекомендації організаційного та технічного характеру (наприклад, розробляти спеціальні технічні пристрої), спрямовані на припинення конкретного злочину, попередження злочинів та інших правопорушень, аналогічних розслідуваному [183, с. 123].

З цього виходить, що, окрім виявлення причин та умов, що сприяли вчиненню комерційних інтернет-шахрайств, фактично до профілактики таких

кримінальних правопорушень слід віднести й діяльність, що перешкоджає вчиненню кримінальних правопорушень.

Цікавою є позиція П. Біленчука, який класифікує засоби криміналістичної профілактики за видами профілактичних завдань на п’ять груп:

1) технічні засоби і методи, що використовують для виявлення фактів, які сприяли вчиненню або приховуванню злочинів;

2) технічні засоби і методи захисту різних об’єктів від злочинних посягань, наприклад, засоби охоронної сигналізації, засоби, які перешкоджають (заважають) вчиненню злочину;

3) технічні засоби, що створюють умови виникнення на місці вчинення злочину додаткових слідів, наприклад, рук, звуку, запаху;

4) технічні засоби і методи отримання інформації про злочини, що готуються (засоби спеціальної техніки, що застосовують правоохоронні органи під час ОРД;

5) технічні засоби і методи справляння активного психологічного впливу на осіб, схильних до вчинення правопорушень (використання телевізійних систем слідкування, установлених у місцях скупчення людей (аеропортах, вокзалах, банківських установах, магазинах тощо). [15, с. 72-73].

Разом з тим, Г. В. Захарова, аналізуючи такий підхід, наголошує, що лише технічними засобами навряд чи можна досягти мети у вирішенні завдань щодо попередження, припинення злочинів, а також виявити всі причини та умови, що сприяють вчиненню злочинів. Адже, виконуючи профілактичну функцію, правоохоронні органи, окрім техніко-криміналістичних засобів, застосовують й організаційно-тактичні заходи [63].

Втім, як на нашу думку, у припиненні та запобіганні комерційних інтернет-шахрайств, саме технічними засобами можна вирішити низку тактичних завдань. До того ж, як показав аналіз юридичної літератури,

вивчення судово-слідчої практики та опитування респондентів, саме 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.

Деякими авторами запропонований навіть алгоритм, за яким виконується процес виявлення шахрайських операцій з боку банківських співробітників, які передають інформацію до правоохоронних органів. Зокрема, фільтрування платежу здійснюється за 3 критеріями, верифікація у випадку необхідності та зберігання результатів в базі даних. Автоматична система починається з форми онлайн-платежу, яку заповнює клієнт. Після цього методом POST дані відправляються до системи з фільтрами для виявлення шахрайських операцій. Кожен фільтр зберігає причину класифікації платежу як шахрайського, якщо вона є. Перший рядок розраховує скільки годин пройшло з моменту останнього платежу. Другий рядок повертає географічні координати поточного місцезнаходження. Далі записується у змінні координати місцезнаходження у момент останнього платежу та поточного місця. Внаслідок чого викликається власна функція calculateTheDistance, яка розраховує відстань між містами у кілометрах. Далі перевіряється, чи достатньо було часу для проходження розрахованої відстані при швидкості у 50 кілометрів за годину. Якщо часу недостатньо, то записується, що платіж шахрайський. Після виконання аналізу за допомогою 3 фільтрів, повертається результат про те, чи є операція шахрайською. Якщо система класифікує її такою, то перевіряється достовірність клієнта – звіряються дані платежу з «білим списком» та відправляється клієнту СМС з кодом. Після введення отриманого коду у форму, платіж підтверджується і клієнт повертається до початкової сторінки оформлення платежу. Для зменшення надмірного відправлення СМС клієнтам з метою додаткової верифікації створюється «білий список». Він являє собою перелік унікальних банківських карт та IP-адрес, операції за якими спочатку були виявлені як шахрайські, але потім пройшли верифікацію. Він формується динамічно

запитом до бази даних. Після виконання алгоритму інформація зберігається в базі даних. Операції які позначені, або були позначені як шахрайські виводяться в додаток, який використовує співробітник банку. Перша частина створена для клієнтів електронної комерції, які хочуть здійснити платіж за допомогою кредитної картки. У своєму браузері клієнт буде бачити форму, в якій йому необхідно заповнити дані про банківську картку та адресу доставки товару. Після натискання кнопки виконується алгоритмічна частина додатку, в якій перевіряється чи є даний платіж шахрайським. Якщо у системи немає зауважень до цього платежу, то транзакція передається на виконання у платіжну систему, а клієнт повертається на початкову сторінку магазину електронної комерції. У випадку виявлення шахрайства виконання транзакції призупиняється і виконується запит до SMS API Service. Співробітник банку отримує перелік всіх платежів за участі свого банку, які були визначені як шахрайські операції, побачить прізвище та ім’я клієнта, картковий рахунок, телефон, дату проведення платежу, причину визначення його як шахрайського та поточний статус [72].

Як свідчить практика, заходи технічного характеру здебільшого поєднуються із організаційними та правовими чинниками.

Деякі автори, з метою профілактики шахрайства, навіть розробили концептуальну модель виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу. Зокрема, виходячи з аналізу статистичних даних можна виділити показники, що можуть вказувати на можливе виникнення кіберзагрози в процесі виконання банківської операції:

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

інтернет-банкінгу та привласнюючи чужі кошти, застосовують спеціальні програми для шифрування їх місцеположення;

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

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

- обнуління рахунків клієнтів банку вказує на ймовірні ознаки кіберзагроз. Сьогодні досить розповсюдженими є безготівкові розрахунки, коли платежі відбуваються без використання готівкових коштів. Тому, в більшості випадків на банківському рахунку людини завжди присутня певна сума коштів. Якщо під час транзакції зі зняття всієї суми можливо має місце ознака порушення користування рахунком або несанкціоноване зняття коштів [219; 228].

Серед заходів криміналістичної профілактики під час розслідування шахрайства необхідно згадати про загально соціальне запобігання. Так, на думку окремих авторів, це позитивний вплив, цілеспрямована реалізація продуманої соціальної політики, яка здійснюється не лише і не стільки з метою безпосереднього попередження економічної злочинності. Вона спрямована передусім на вирішення загальних економічних і соціальних завдань держави. Загальносоціальне запобігання економічній злочинності полягає в тому, що його здійснення зменшує вплив соціальних суперечностей, нейтралізує криміногенне протистояння різних верств населення, рівень безробіття, підвищує стандарт життя людей, створює

необхідні умови для легалізованого одержання достатніх прибутків громадянами, сприяє побудові міцного фундаменту щодо нормального функціонування всіх соціальних сфер, впровадження високих моральних цінностей у ньому, додержання демократичних засад тощо. Прогресивні соціальні програми спрямовані на утвердження законності, поваги до конституційних прав і свобод людини, зміцнення громадського порядку, дисципліни, на вирішення проблем поєднання громадських, виробничих, сімейно-побутових інтересів, соціальної адаптації маргінальних верств населення тощо[43, с. 85].

До загально соціальної профілактики можна віднести й повідомлення в ЗМІ із висвітленням проблем комерційних інтернет-шахрайств та шляхів запобігання ним.

Так, найпопулярнішими заходами щодо запобігання шахрайствам в Інтернеті з боку громадян є:

- щодо послуг перевезення: громадянам слід намагайтеся купувати квитки та бронювати місця в офіційних перевізників та не надавати передоплату. Обов’язково слід перевіряти репутацію перевізника шляхом пошуку відгуків;

- щодо послугпошуку житла: громадянами слід вимагати додаткові детальні фото приміщення та не вносити передплату без фактичного заселення;

- щодо внесків на адресу благодійних фондів чи волонтерів: громадянам слід перш за все перевірити історію цих організацій;

- при купівлі будь-яких товарів в мережі Інтернет, в тому числі для армії: громадянам слід не відправляти передоплату та здійснювати відправку товарів накладним платежем;

- громадянам слід перевіряти гіперпосилання та наповнення сайту на відповідність офіційним даним компаній та не вказувати власні персональні дані на неперевірених сайтах, а також нікому не повідомляти термін дії банківської карти та CVV-код.

У будь якому випадку обов’язково слід звертатися до органів Національної поліції чи направляти звернення на електронну скриньку Сервісної служби кіберполіції «callcenter@cyberpolice.gov.ua.». До того ж, в інтернеті існує відкрита база шахраїв на кшталт https://marker.org.ua/base/fake-olx, де громадяни можуть перевірити відгуки інших покупців та поділитися своїм досвідом[212].

Профілактична функція насамперед стосується й оперативних підрозділів кіберполіції. Зокрема, Департамент кіберполіції відповідно до покладених на нього завдань:

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

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

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

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

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

- відповідно до чинного законодавства збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінює результати за окремими показниками службової діяльності, надає, відповідно до законодавства України, звіти про результати роботи та відповідну інформацію керівництву Національної поліції України, МВС, органів державної влади з питань попередження та протидії кіберзлочинам [9, с. 92; 144].

Загалом попередження та протидія комерційним кібершахрайствам поєднує ряд заходів правового, соціального, технічного, організаційного та інформаційного характеру.

На наш погляд, досить успішно втілює заходи правового, соціального, технічного, організаційного та інформаційного характеру І. О. Коновалова.

Серед заходів запобігання електронному комерційно-торгівельному шахрайству в Україні, вчена виділяє наступні:

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

- запровадження політики належного корпоративного управління;

- упровадження дієвих законодавчих ініціатив щодо належного регулювання комерційної реклами та / або просування комерційних продуктів або послуг; встановлення кримінальної відповідальності за злом та крадіжку в мережі, знищення приватної та / або секретної інформації;

- реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство;

- використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства;

- популяризації електронної комерції через он-лайн та оф-лайн магазини;

- посилення міжнародного співробітництва та залучення громадськості до соціально-виховної роботи з профілактики шахрайства в сфері електронної торгівлі [80].

А. Б. Мізерак, досліджуючи шахрайство при інтернет-торгівлі, робить акцент саме на правових аспектах запобігання таким проявам.

Зокрема, з метою запобігання таким проявам вчений пропонує вдосконалити правові відносини, що виникають в процесі бізнесу з використанням глобальної мережі Інтернет, для чого є необхідним:

- сутнісне визначення та законодавче закріплення деривації «віртуальний простір», категорій «інтернет-суспільство», «інтернет-відносини», «інтернетзлочинність»;

- актуалізація законодавчих актів, що регулюють інтернет-відносини;

- законодавче визначення класифікації інформаційних прав громадян у мережі Інтернет-магазинів, з'ясування характеру та особливостей правозастосування юридичних норм, що регулюють діяльність користувачів цієї мережі в Україні;

- законодавче визначення меж державного втручання у суспільні відносини, пов'язані з використанням мережі Інтернет-магазинів;

- розширення дій кримінальної відповідальності за злочин у мережі Інтернет - магазин ;

- посилення відповідальності адміністраторів баз даних та інших осіб, які забезпечують експлуатацію комп'ютерних інформаційних систем та діяльність [110].

Н. І. Костова до основних напрямів стимулювання розвитку вітчизняного ринку електронної комерції відносить такі: узгодження правових норм укладення угод в електронному вигляді; забезпечення державного сприяння розвитку електронної комерції для усунення перешкод для здійснення електронних операцій, недопущення будь-яких форм дискримінації, надання учасникам рівних прав на судовий захист; поширення інформації та здобуття знань суб’єктами господарювання про можливості

електронної комерції та переваги для бізнесу в разі їх впровадження; розбудова інфраструктури ринку електронної комерції [84, с. 74].

О. Л. Андронік та А. В. Воронін також акцентують, що електронна комерція в Україні потребує внесення відповідних змін до чинного законодавства, а саме: врегулювання питання відповідальності власників маркетплейсу перед споживачем за недобросовісні дії сторонніх продавців; впровадити механізм швидкого блокування недобросовісних суб'єктів електронної комерції; визначити чіткі правила розміщення інформації про продавця з можливістю «підтягування» даних з Єдиного державного реєстру юридичних та фізичних осібпідприємців та громадських формувань; для мінімізації втручання державних інституцій у стосунки між споживачами та суб'єктами господарювання та зниження адміністративного тиску на бізнес, запровадити механізми досудового врегулювання спорів між споживачами та продавцями; створити відповідний реєстр електронної комерції, з обов'язковою реєстрацією у ньому суб'єктів електронної комерції [2, с. 127].

Важливим є й зарубіжний досвід запобігання комерційним інтернет-шахрайства.

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

- регулярний аудит безпеки сайту щодо: оновлення програм для кошика покупок; актуальності та дієвості роботи сертифіката SSL; відповідності магазину стандарту безпеки даних індустрії платіжних карток - PCI-DSS; наявності резервної копії магазину; надійності паролів для облікових записів адміністраторів, панелей керування хостингом, бази даних та доступу по FTP; сканування веб-сайту на наявність шкідливих програм та ін.;

- відповідність онлайн-магазину стандарту PCI DSS. Інтернет-магазин, який приймає платежі за кредитними картками, повинен відповідати вимогам

PCI DSS - стандарту безпеки даних індустрії платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованою міжнародними платіжними системами Visa, MasterCard, American Express, JCB та Discover. Стандарт являє собою сукупність деталізованих вимог щодо забезпечення безпеки даних про власників платіжних карток, які передаються, зберігаються та обробляються в інформаційних інфраструктурах організацій. Прийняття відповідних заходів щодо забезпечення відповідності вимогам стандарту представляє комплексний підхід до забезпечення інформаційної безпеки даних платіжних карток [80, с. 221].

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

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

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

- використання безпечного протоколу передачі гіпертексту (HTTPS) - протоколу, який забезпечує цілісність та конфіденційність даних при їх передачі між сайтом та пристроєм користувача, який передбачає три основні рівні захисту: шифрування переданих даних; цілісність даних; та

аутентифікацію, яка гарантує, що відвідувачі потраплять саме на сайт, який їм потрібен, окрім цього, захищає від атаки посередника[80, с. 224];

- зберігання обмеженої кількості інформації. Один зі способів захистити онлайн-магазин від витоку даних чи злому – зберігати якомога менше даних про клієнтів, адже, хакери не можуть вкрасти те, чого немає. Тому онлайн-магазинам рекомендується збирати та зберігати лише дані, необхідні для завершення транзакції та відправлення продукту, при цьому уникати збирання номерів соціального страхування, дат народження та інших непотрібних конфіденційних даних клієнтів [226; 115];

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

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

- використання програм для боротьби з шахрайством, серед яких: Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone, Precognitive, SEON, FraudLabs Pro. Відповідні програми при оплаті автоматизують перевірки на шахрайство, здійснюють блокування підозрілих пристроїв, скасування шахрайських замовлень та багато іншого [80, с. 223; 227].

Вказане свідчить про необхідність поглиблення практичної складової міжнародного співробітництва з питань боротьби з кіберзлочинністю взагалі та кібершахрайством зокрема в частині оперативного обміну інформацією. Важливим є обмін інформацією між оперативними підрозділами різних країн про багатоепізодні кібершахрайства, що вже вчинені чи готуються. Найкращим способом боротьби, найефективнішим для будь-яких видів злочинів є його недопущення, попередження, виявлення при цьому причин і умов, які сприяють його вчиненню, їх обмеження, нейтралізація, усунення, а вже потім – розкриття [211, с. 189].

У системі тактичних заходів з усунення причин злочинності особливо актуальною є профілактика суспільно небезпечних діянь з участю засуджених [100, с. 472],Необхідність здійснення даного виду запобігання злочинам

обумовлена, зокрема, наявністю в УВП віктимологічної криміногенної ситуації [100, с. 472].

Ця думка має право на своє існування, адже, як показав аналіз кримінальних проваджень щодо комерційних інтернет-шахрайств, 12 % таких випадків вчиняється саме з місць позбавлення волі. Як правило, неналежний нагляд за засудженими з боку персоналу УВП та корупційна складова сприяють тому, що у більшості в'язнів є можливість користуватися засобами мобільного зв'язку та Інтернетом. Завдяки чому вони безперешкодно можуть ошукувати громадян навіть у дистанційній формі.

У цьому розрізі М. М. Яцишин, ретельно вивчаючи питання профілактики злочинів з боку засуджених в установах виконання покарань, пропонує заходи щодо усунення, нейтралізації чи компенсації зовнішніх умов злочинності в УВП, зокрема:

- конструктивно-технологічна розробка принципово нових засобів комп'ютерного збору, обробки та використання інформації про конкретні колонії по напрямках їх діяльності, засоби охорони й нагляду за засудженими, ефективність засобів цілодобового спостереження за засудженими, технічних засобів перевірки посилок, передач, листів, огляду автотранспорту, обшуків засуджених та їх речей і т. д.;

- комплексні профілактичні операції в колонії, що пов'язані з мобілізацією усіх сил і засобів УВП, а при необхідності – залучення можливостей сусідніх колоній, у тому числі інших областей і регіонів;

- організація оперативного обміну інформацією між різними службами УВП про криміногенні ситуації, угрупування антисуспільної спрямованості серед засуджених та їх вірогідні акції тощо;

- підвищення дисциплінованості персоналу УВП, організація правильної дисциплінарної практики, коли крайні заходи реагування до порушників дисципліни з боку адміністрації колонії застосовуються після використання інших, більш м'яких, стягнень, передбачених Дисциплінарним Статутом тощо [221].

Отже, підбиваючи підсумки, можна виділити наступні найбільш поширені заходи з профілактики комерційних інтернет-шахрайств, зокрема:

- розміщення оголошень в ЗМІ щодо способів комерційних інтернет-шахрайств та заходів їх запобігання;

- виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу;

- відслідковування операцій, які потенційно можуть бути шахрайськими з урахуванням кількості карток клієнта, його місцезнаходженням та місцем здійснення операції, місцезнаходженням та адресою доставки, тощо;

- використання новітніх електронних систем та 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 та пристроїв;

- підсилення міжнародного співробітництва у боротьбі із 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 в сфері електронної торгівлі тощо.

3.3. Застосування тактичних операцій під час розслідування шахрайства в інтернет-комерції

Під час розслідуванняшахрайства в інтернет-комерції виникає низка тактичних завдань, які під силу вирішити тільки за умов застосування комплексу слідчих (розшукових) та негласних слідчих (розшукових) дій, процесуальних, організаційних та оперативно-розшукових заходів. У криміналістичній літературі такий комплекс називається тактичною операцією.

Хоча, як зауважує А. М. Чорний, на практиці криміналістичні комплекси у вигляді тактичних операцій використовуються ще досить рідко, слідчі замість нихвіддають перевагу послідовному проведенню окремих слідчих дій, які за своїм призначенням ічасом проведення нерідко порушують логіку пошуку доказів, які підтверджують висунуту версію. Послідовність проведення окремих слідчих (розшукових) дій нерідко спричиняє втрату інформації,створює часовий потенціал для злочинців, використовуваний для приховування або знищеннядоказів, залякування свідків, придумування неправдивих алібі тощо. У цьому аспекті проведення тактичних операцій сприяє не тільки швидкості одержання необхідної інформації, але й усуненню перешкод, які створюються для її одержання [2-3, с. 238].

На думку В. М. Шевчука, тактичні операції мусять мати видову і підвидову спрямованість. Автор наводить таку систему типових тактичних операцій: 1-ий рівень утворюють типовівидові тактичні операції, які відбивають специфіку саме певного виду злочинів (наприклад, вбивства, шахрайства); 2-ий рівень утворюють типові-підвидові (предметні) тактичні операції, які створюються відповідно до конкретного різновиду злочинів [214, с. 256; 213].До того ж, слід погодитися із тими авторами, які вважають, що процес розслідування стає найбільш оптимальним, якщо проводиться не одна, а кілька тактичних операцій, що дозволяють не тільки успішно вирішити проміжні завдання, а й максимально наблизитися до досягнення кінцевої мети розслідування. Зміст і спрямованість тактичної операції обумовлені, по-перше, слідчою ситуацією, а по-друге, видовими особливостями розслідуваного злочину [198].

Завданням дослідника при побудові окремої методики розслідування є визначення типового кола таких проміжних завдань і розроблення відповідних рекомендацій щодо організації і проведення типових тактичних операцій [173, с. 204].Наприклад, Р. Л. Степанюк до найтиповіших тактичних завдань розслідування кримінальних правопорушень відносить такі, як: 1) затримання підозрюваного; 2) пошук інформації про можливих співучасників і роль кожного з них; 3) розшук підозрюваного, що переховується; 4) виявлення ознак інших кримінальних правопорушень, пов'язаних із розслідуваним; 5) виявлення корумпованих зв'язків; 6) нейтралізація протидії розслідуванню; 7) забезпечення збереження документів, що мають значення для розслідування як джерела доказової інформації; 8) забезпечення відшкодування заподіяної кримінальним правопорушенням шкоди; 9) виявлення і припинення кримінальних правопорушень, що готуються або продовжуються; 10) запобігання можливому вчиненню кримінального правопорушення; 11) встановлення причин і умов, що сприяли вчиненню кримінального правопорушення, і вжиття заходів щодо їх усунення тощо [169, с. 145].Натомість, ряд вчених, окрім типових, виділяють ще й індивідуальні завдання. У цьому розрізі К. В. Латиш, із урахуванням нерозривного зв'язку тактичних завдань та тактичних операцій, пропонує виділити таку трьохчленну концепцію тактичних проміжних (локальних) завдань під час розслідування: пізнавальні, діагностичні та пошукові тактичні завдання, вирішенню яких кореспондують відповідні тактичні операції [98, с. 115].

Переходячи до визначення тактичних завдань під час розслідування шахрайства в інтернет-комерції, слід сказати, що ряд локальних завдань спрямовано на: виявлення шахрайських операцій шляхом перевірки за різними фільтрами; перевірку історії проведених транзакцій; встановлення місцезнаходження точки доступу до інтернету та провайдера, який сприяв доступу до мережі інтернет; отримання інформації, що міститься у поштовій скринці; встановлення справжності чи фіктивності інтернет-сайтів;

встановлення шахрайського умислу та виключення форсмажорних обставин, що не надали можливість виконати договірні зобов'язання тощо.

Виходячи з окреслених завдань розслідування, можна запропонувати такі типові тактичні операції: «Злам аккаунта та проведення незаконної транзакції», «Встановлення IP-адреси», «Ідентифікація особи у віртуальному просторі», «Фальшивий сайт», «Встановлення умислу», «Організація затримання шахрая, який діяв в мережі інтернет» тощо.

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

Важливу роль у реалізації такої тактичної операції відіграє Департамент кіберполіції, який надає істотну допомогу органам досудового розслідування та підрозділам карного розшуку у виявленні та доведенні фактів шахрайства у мережі Інтернет.

Так, протиправну діяльність зловмисників викрили співробітники управління протидії кіберзлочинам у Харківській області спільно зі слідчим управлінням обласної поліції. Для реалізації злочинних намірів фігуранти створили та адміністрували скам-спільноту в месенджері «Телеграм», в якій розміщували інструкції та фішингові посилання для інших членів шахрайської організації. Далі зловмисники в месенджерах робили розсилку фішингових посилань, що містили пропозицію отримати соціальну допомогу від держави або отримати кошти за проданий товар. Після введення потерпілим реквізитів своєї банківської карти, зловмисники отримували доступ до його коштів.За оперативною інформацією, підозрювані ошукали понад 300 потерпілих та завдали близько одного мільйона гривень збитків. За місцями проживання фігурантів працівники поліції провели обшуки.

Вилучено ноутбуки, мобільні телефони, банківські картки, гроші. До проведення обшуків також були залучені працівники полку поліції особливого призначення. Організатора та ще двох виконавців затримано за ст. 208 КПК України. Організатору повідомлено про підозру за ч.1, ч.2 ст.255 (створення та участь у злочинній організації), ч.4 ст. 28, ч. 3 ст. 190 (шахрайство) Кримінального кодексу України. Виконавцям - за ч.2 ст.255, ч.4 ст. 28, ч. 3 ст. 190 Кримінального кодексу України [136].

У цьому розрізі слід зауважити, що нерідко, коли відбувається шахрайське придбання, банківські рахунки, на які надходять кошти, знаходяться в різних країнах ЄС або за кордоном. У тих випадках, коли банки перебувають за межами ЄС, розслідуваннюможуть сприяти схеми міжнародних карток. Багато веб-сайтів та облікових записів у соціальних мережах використовуються для шахрайського створення інтернет-магазинів або придбання електронних товарів. Оборот підозрюваних може сягати мільярдів євро по всьому світу щороку. Шахраї використовують вкрадені дані кредитних карток, отримані в даркнеті, за допомогою шкідливих програм або фішингових атак для купівлі товарів. Споживачі іноді не усвідомлюють, що дані їх картки також вкрадені або скомпрометовані, коли вони купують. Промисловість, банки та торговці мають бути оштрафовані і ті, хто зафіксував вищі збитки [222].

З метою виявлення таких фактів обираються найважливіші дані з урахуванням обсягу та частоти процесів. Важливо визначити підмножину інформації, що дозволить добре сформулювати модель даних та всі підсистеми. Система виявлення шахрайських операцій складається з наступних складових (підсистем): – Fraud Predictor Service – сервіс виявлення шахрайських операцій за допомогою перевірки за різними фільтрами; – Transactions Log – база даних транзакцій банківських карт; – SMS API Service – сервіс верифікації за допомогою повідомлення на мобільний телефон. Крім того система містить клієнтські веб-додатки як, наприклад, вебдодаток для

банку для відображення транзакцій, котрі система визначила шахрайськими [72, с. 148].

Під час проведення тактичної операції, спрямованої на виявлення незаконних транзакцій, всю інформацію, що підлягає встановленню, слід поділити на три групи: інформація, яку вводить клієнт; інформація, яка зберігається у системі (історія транзакцій); інформація, що виводиться співробітнику банка.

При виконані операції з певної IP-адреси, програма визначає зі скількох інших банківських карт виконувалися онлайноперації за останню добу. Якщо унікальних карт буде більше двох, то операція вважається шахрайською.Робота даного фільтру полягає у порівнянні поточного регіону та міста, яке визначається за IP-адресом та місто, в яке замовлено доставку товару. У випадку різних значень додатково перевіряється, чи куплялися товари раніше на ту адресу. Якщо дана адреса вже була збережена у транзакціях клієнта, то операція не вважається шахрайською.Одночасно на апаратних засобах правопорушника працює додаток-сніффер, активована точка доступу Wi-Fi з ім’ям, схожим чи ідентичним до назви точки доступу закладу або місця. Коли звичайний користувач підключається до однієї з наявних загальнодоступних мереж, він може стати потенційною жертвою зловмисника. Весь транзитний трафік перехоплюється сніффером, і піддається аналізу щодо імен і паролів користувача платіжних систем, номерів кредитних карт, паролів підтвердження оплати тощо. Фактично перехоплюється весь трафік, але за умови, що жертва підключилась саме до псевдомережі шахрая[153, с. 86].

Шахраї, зазвичай, намагаються здійснювати певні дії для своєї анонімності. Під час отримання грошей шахраїв крім анонімності рятує ще й швидкість, адже переказ отриманих коштів між різними платіжними системами здійснюється досить швидко, але вимагає багато часу для відстеження. Натомість, здійснення шахрайських операцій передбачає залишення великої кількості слідів технічного характеру [151, с. 53].

Вивчення судово-слідчої практики та анкетування працівників Національної поліції, які мали відношення до розкриття та розслідування шахрайства в інтернет-комерції, дозволило встановити, що у 92 % випадків під час розслідування таких кримінальних правопорушень виникає необхідність щодо встановлення точок доступу, з яких здійснювалися шахрайські дії та ідентифікації особи, яка мала відношення до шахрайства. У зв'язку із чим стають в нагоді такі тактичні операції, як «Встановлення IP-адреси» та «Ідентифікація особи у віртуальному просторі».

У цьому розрізі слід зауважити, що кожне замовлення, розміщене в інтернет-магазині, надходить з унікальної загальнодоступної IP-адреси. За IP-адресою, зазвичай, можна визначити місто чи регіон світу де споживач здійснює покупку. Якщо це місто чи регіон не збігається з адресую кредитної картки, яка використовується, це може означати загрозу шахрайству. Використання програм для боротьби з шахрайством. Коли справа доходить до виявлення та запобігання шахрайству в електронній торгівлі, існує безліч програмних рішень, які відповідають різним потребам та бюджету. Прості програми боротьби з шахрайством виконують специфічну функцію. Зазвичай, вони інтегровані в онлайн-кошики та платформи електронної комерції. Ці інструменти використовують алгоритми машинного навчання для виявлення шахрайських транзакцій за допомогою геолокації IP, перевірки адрес електронної пошти, проведення відбитків пальців пристрою та перевірки адрес. Програми для боротьби з шахрайством середнього рівня пропонують більш широкий спектр функцій, включаючи гарантії повернення платежів, автоматичне відхилення замовлень із високим ризиком, захист від нових шахрайств з обліковими записами та захист від поглинання облікового запису. Програми найвищого рівня захисту виконують всі ті ж функції, що й вищезазначені програми, а також пропонують аутсорсингове управління справами, роботу з великими продавцями, управління шахрайством із лояльністю, захист від зловживання політикою, автоматичне прийняття рішень та ручний перегляд підозрілих транзакцій, гарантуючи, що жодне

хороше замовлення не буде помилково відхилено програмним забезпеченням. Відповідні програми при оплаті автоматизують перевірки на шахрайство, здійснюють блокування підозрілих пристроїв, скасування шахрайських замовлень та багато іншого [80, с. 223; 227].

В рамках тактичної операції, з метою встановлення належності електронної поштової адреси та встановлення особи, яка користується відомою адресою, необхідно за допомогою сервісу Whois визначити провайдера, який надає послуги використання електронної пошти, і звернутися до нього із запитом (чітки позиції запиту [154, с. 24]. При цьому, номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор по визначенню входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання. Саме тому, завдяки наявності IP-адреси особи, яка представляє оперативний інтерес, можливо встановити місцезнаходження точки її доступу до Інтернету (країну, місто), та назву провайдера, який надає особі можливість такого доступу до Інтернету. Головним завданням, в даному випадку, виступає спосіб отримання IP-адреси особи, яка представляє оперативний інтерес. Основними способами є такі, як: запити до адміністрації звичайних (комерційних чи некомерційних) Інтернет-сайтів та використання легендованих Інтернет-сайтів [105, с. 63].

Типовими є ситуації, коли шахраї створюють на сторінках Інтернет – аукціонів декількох користувачів, які мають різні особисті данні та імена профілів. Також шахраї можуть створювати декілька різних профілів у різних сервісах по продажу товарів через мережу Інтернет, чи по продажу товарів на сторінках Інтернет – аукціонів. За допомогою цих профілів, шахраї створюють сторінки по продажу товарів, але оскільки дуже часто реального товару на руках у шахраїв немає, вони використовують однакові графічні

зображення, чи цифрові фотографії товару для створення оголошення. Крім того, як правило, шахраї використовують відносно одні й ті самі міні-зображення для своїх профілів – так звані «аватарки». Працівникам ОВС вкрай необхідно мати у розпорядженні якомога більше інформації про ту, чи іншу особу, яка представляє оперативний інтерес. А тому пошук в мережі Інтернет усіх створених оголошень та профілів конкретної особи може принести працівникам ОВС багато значимої інформації. Для реалізації принципу «більша кількість даних створює більшу кількість даних, знайдених з її допомогою», шляхом пошуку ідентичних зображень в мережі Інтернет, необхідно скористатися послугами, що представляють Інтернет сервіси трьох типів: звичайні пошукові сервіси, вбудовані доповнення у звичайні пошукові сервіси, та спеціальні сервіси по пошуку графічних зображень [105, с. 53-54].

Окільки шахраї використовують комп'ютерну техніку, у тому числі для підготовки проектів різних підроблених документів, зберігання відео- або фотофайлів, ведення переговорів в мережі Інтернет і електронною поштою, відвідування соціальних мереж, в пам’яті комп’ютера можуть бути адреси потенційних жертв, графічні зразки бланків та інша важлива інформація. На флеш-карті мобільного телефону також може зберігатися значна кількість інформації про контакти, зв'язки тощо. Тому така інформація, безсумнівно, становить інтерес для слідства та спрямовує правоохоронні органи у вірному напрямку [148, с. 135].

Тактичні операції «Встановлення IP-адреси» та «Ідентифікація особи у віртуальному просторі» передбачають такі поступові слідчі (розшукові) дії, оперативно-розшукові й організаційні заходи:

- зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов’язаний з подоланням системи логічного захисту;

- встановлення місцезнаходження радіоелектронного засобу;

- оформлення та відправлення запитів про витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових осіб відомостей, що становлять інтерес для кримінального провадження та/або здійснення запитів щодо обміну інформацією між компетентними підрозділами правоохоронних органів іноземних держав з питань реагування на кіберзлочини каналами сектору Національного контактного пункту реагування на кіберзлочини (НПК ДКП НП України) [154, с. 35];

- допити потерпілих та свідків;

- обшуки у підозрюваних;

- огляд комп'ютерної техніки;

- призначення експертиз тощо.

Переходячи до тактичної операції «Фальшивий сайт», слід сказати, що вітрина Інтернет-магазина розташовується на Інтернет-сервері та являє собою Web-сайт із активним вмістом.

Web-сайт (система електронної комерції) – це сукупність технічних засобів, програмних продуктів і методів для реалізації в автоматизованому режимі технологічних процесів у певній комерційній операції. Web-сайт – це сполучена під однією адресою (доменне ім'я або IP адреса) сукупність документів фізичної особи або підприємства. Сукупність усіх сайтів складає Всесвітню павутину. На сьогоднішній день з урахуванням тенденцій розвитку мережі Інтернет існує досить велика кількість різних Web-сайтів, які досить сильно відрізняються один від одного. Сучасні системи CMS переважно використовуються для створення будь-яких сайтівта електронних магазинів (Інтернет-магазинів) [194, с. 15-17].

Через те, що Інтернет-магазин повинен мати постійний зв'язок з інформаційною системою компанії, він розміщується або на корпоративному сервері в локальній мережі підприємства, або на вилученому сервері з постійно діючим каналом зв'язку. Необхідність повної автоматизації бізнес-процесів компанії визначає високі вимоги до системи керування

процесами бэк-офіса, тому без допомоги фахівця слідчому впоратися дуже складно. Ця система повинна забезпечувати автоматичне виконання усіх дій, пов'язаних з продажами, складськими операціями, мати внутрішні механізми контролю позаштатних ситуацій і т.д. У загальному випадку, мінімальний набір апаратно-програмних компонентів, який необхідний для роботи Інтернет-магазина, включає: Web-сервер – розподіляє запити, які надходять з Інтернету, здійснює‒ розмежування доступу до інформації; Сервер додатків – керує роботою торговельної системи, зокрема‒ бізнес-логікою Інтернет-магазина; СКБД-сервер – забезпечує зберігання та обробку даних про товари,‒ клієнтів, рахунки й т.д. [194, с. 36].

При огляді веб-сторінки сайта, слід враховувати наступні моменти. Так, необхідно, щоб на сайті були витримані: − єдині стандарти фірмового стилю (єдина символіка, кольорова гама, прийоми верстки, фірмові персонажі); − грамотна манера написання текстів, їх характер (єдиний стиль, жанр); − корпоративні стандарти обслуговування клієнтів (дотримання ціннісних орієнтирів, певної манері спілкування, швидкість реагування, обрання пріоритетів). Усі перераховані інструменти брендингу повинні підсилювати один одного, тим самим створюючи загальний образ компанії, підтримуваний сайтом. При адаптації фірмового стилю до застосування на Web-сайті: − логотип компанії має розташовуватися нагорі усіх сторінок, не повинен бути викривлений або зіпсований; − навколо логотипа мають бути залишені стандартні поля (так звана «захисна зона», розміри якої зазвичай пропорційні самому логотипу); − слоган компанії повинен розташовуватися у помітному місці і відтворюватися абсолютно точно; − якщо в компанії є фірмовий персонаж, то його зображення може бути присутнім на сайті; − при підборі ілюстрацій необхідно дотримуватися іміджевої політики компанії (наприклад, використовувати певні фотографії, піктограми, іконки); − на сайт можуть бути в адаптованому вигляді перенесені деякі прийоми форматування тексту, характерні для фірмової поліграфії (наприклад, способи оформлення заголовків, цитат, виносок тощо); − невелике зображення, що виводиться в

адресний рядок браузера (англ. – favicon, скор.від англ. FAVorites ICON – «значок для обраного»), повинно бути намальовано з урахуванням фірмової символіки компанії і повторювати її фірмовий знак [217, с. 44].

Якщо в ході проведення огляду у правоохоронців виникнуть сумніви щодо справжності сайту інтернет-магазину, можна розраховувати на виявлення таких слідів:

- реєстраційні дані на доменне ім'я;

- логи від взаємодії з реєстратором доменних імен;

- сліди від проведення платежу цього реєстратора;

- сліди при налаштуванні DNS-сервера, що підтримує домен шахраїв;

- сліди від взаємодії з хостинг-провайдером, у якого розміщений веб-сайт: замовлення, оплата, настройка контенту;

- сліди від рекламування веб-сайта: взаємодія з рекламними майданчиками, системами банерообміну, розсилка спаму;

- сліди від відстеження активності користувачів на сайті тощо.

- при взаємодії з жертвами обману шахраї залишають сліди при прийомі замовлень – по електронній пошті, через СМС повідомлення, через ICQ, або веб-форму;

- від листування з потенційними жертвами. При отриманні грошей шахраї залишають сліди при здійсненні введення грошей в платіжну систему (реквізити, які вказуються жертві);

- при переказі грошей між рахунками, які контролюються шахраями;

- сліди при виведенні грошей;

- від дистанційного керування шахраями своїми рахунками, їх відкриття і закриття;

- від взаємодії шахраїв з посередниками з відмивання і переведення грошей у готівку [151, с. 53].

Для встановлення належності сайту за допомогою сервісу Whois визначається провайдер, який надає послугу хостингу. Далі для встановлення належності сайта необхідно звернутися до провайдера із запитом про:

реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостингу для сайта; адреси, телефонні номери та інші реквізити власника сайта; IP-адреси, використані для створення сайта; IP-адреси, використані для поповнення сайта; інформація про зміст сайта; інформація про користування сайтом [154, с. 24].

Тактична операція «Фальшивий сайт», окрім окреслених заходів, включає ще й: зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту; встановлення місцезнаходження радіоелектронного засобу; допити потерпілих та свідків; огляд комп'ютерної техніки; призначення експертиз тощо.

Щодо тактичної операції «Організація затримання злочинця, що діє в мережі Інтернет», слід сказати, що у випадку, коли підозрювані у шахрайстві особи намагаючись уникнути кримінального покарання переховуються від органів досудового розслідування, то всі слідчі (розшукові) та негласні слідчі (розшукові) дії повинні бути направлені на встановлення місця їх перебування. Для цього, із застосуванням існуючих криміналістичних обліків, та електронних реєстрів особливу увагу слід приділити також з'ясуванню істинних анкетних даних підозрюваних у шахрайстві осіб, з'ясування місця їх реєстрації, та місця фактичного проживання, встановлення кола їх знайомих, та родичів. Встановлення спостереження за місцем можливої появи шахраїв. Направлення запитів щодо встановлення фактів вчинення аналогічних шахрайських дій тощо [65].

Проведення негласних слідчих (розшукових) дій для встановлення місця перебування розшукуваних осіб має специфічну мету, яка відмінна від випадків їх проведення для отримання доказової інформації у кримінальному провадженні. У ході проведення таких дій діяльність правоохоронних органів, перш за все, спрямована на отримання інформації, що може бути використана для встановлення конкретного місця знаходження особи, що

розшукується та його безпосереднього затримання. Варто зауважити, що за результатами проведення негласних слідчих (розшукових) дій у розшуковій роботі слідчого нерідко встановлюється доказова інформація щодо вчинених злочинів, а також факти вчинення інших суспільно-небезпечних діянь, про які не було раніше відомо правоохоронним органам. Кожна із негласних слідчих (розшукових) дій у розшуковій роботі слідчого має специфічне спрямування і за результатами їх проведення може бути отримана різноманітна інформація. В ході проведення аудіо-, відеоконтролю особи (ст. 260 КПК України) можливо отримати таку інформацію: дані щодо фактичного місця проживання розшукуваної особи; номер його мобільного телефону; особливості зв'язку родичів, знайомих із розшукуваною особою тощо. Окрім зазначеного проведення такої дії сприяє отримати інформацію щодо речових доказів та інших доказів, які стосуються вчиненого злочину [99, с. 119].

Окрім вказаних, до тактичного комплексу входять також наступні дії: здійснення за дорученням слідчого оперативним підрозділом заходів оперативного (ініціативного) пошуку з метою встановлення місцеперебування особи; попереднє опитування особи, яку підозрюють; погодження клопотання про застосування запобіжного заходу щодо цієї особи, затримання; повідомлення про підозру й допит підозрюваного [154, с. 36]; допити свідків та потерпілих; проведення судових експертиз тощо.

Тактична операція «Встановлення умислу» передбачає проведення наступних дій та заходів: зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача; контроль за вчиненням злочину у формі спеціального слідчого експерименту; допити потерпілих та свідків тощо.

У зв'язку із тим, що на розгляд слідчого часто надходять різноманітні файли зі звуковими, відеоформатами, вилучені мобільні телефони та комп'ютери підозрюваної або потерпілої особи, через які відбувалося спілкування, в нагоді стає огляд комп'ютерної техніки та електронних носіїв інформації, а також призначення судових експертиз.

Зокрема, в рамках проведення тактичної операції актуальним є проведення експертизи телекомунікаційних систем (обладнання) та засобів. Проте, виконуючи функції цифрового органайзера або персонального комп'ютера (спеціалізованого комп'ютера з відповідним програмним забезпеченням для роботи з електронною поштою, перегляду текстових або мультимедійних файлів тощо), ця техніка одночасно є об'єктом комп'ютерно-технічної експертизи. Мобільні телефони оснащені слотом для карти пам'яті, і їх можна підключити до комп'ютера як звичайний зовнішній накопичувач інформації з файловою системою. Об'єктами цієї експертизи часто є: Інтернет IP вузли, веб-сторінки, приймачі радіосигналів, вузли комутації; первинні мережі зв'язку, наземні станції супутникового зв'язку, обставини (адресації в мережі Інтернет; передачі радіосигналів; використання доменних імен у мережі Інтернет тощо) [154, с. 29].

Встановлюючи наявність умислу шахраїв, слід звернути увагу на Постанову Верховного Суду України від 24 листопада 2016 року, в якій зазначається, що наявність формальних (навіть належним чином оформлених) цивільно-правових відносин, за допомогою яких суб'єкт прагне завуалювати свій злочинний умисел, за наявності підстав не повинна бути перешкодою для оцінки скоєного як злочину, передбаченого статтею 190 КК. Згідно судової практики, дляквалiфікації скоєного як шахрайства не має значення рівень витонченості обману, ступінь обачності або, навпаки, легковажності потерпілого. Важливо лише, щоб у конкретній ситуації потерпілий не усвідомлював факту застосування щодо нього обману (зловживання довірою), щоб обманні дії винного були ефективними в аспекті успішного заволодіння чужим майном (правом на нього). Обов'язковою ознакою шахрайства визнається добровільність передачі майна чи права на нього; щоправда, така добровільність має умовний (уявний) характер, адже насправді дії зазначених осіб щодо передачі майна чи права на нього зумовлені тим, що вони введені в оману. Між діянням винного і помилкою потерпілої особи, яка передає майно, повинен бути причинний зв'язок [139].

Отже, якщо форсмажорні обставини відсутні, і має місце заздалегідь спланований намір обманути потерпілого, йдеться про шахрайство.

Висновки до розділу 3

Констатуючи зазначене у розділі, підсумуємо викладений матеріал таким чином.

1. 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 %.

2. 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 в інтернет-комерції 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 іншої – паперові та електронні документи, а також комп’ютерна техніка можуть виступати речовими доказами у кримінальному провадженні.

3. Успіх проведення допиту залежить від того, наскільки докладно слідчий ознайомиться із матеріалами кримінального провадження та складе уявлення про особу допитуваного. Окрім загальновизнаних елементів підготовки (вивчення матеріалів провадження, вивчення особи допитуваного, обрання місця і часу допиту, підготовка техніко-криміналістичних засобів для

фіксування допиту), слідчий повинен опрацювати й законодавство, що регулює торгівельні правовідносини в режимі онлайн з 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 установлення автентичності в онлайн-режимі тощо.

4. Значну увагу у провадженнях щодо шахрайств в інтернет-комерції відіграють НСРД, 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).

5. Серед основних профілактичних заходів є виявлення причин і умов, що сприяють учиненню шахрайств, а також застосування заходів щодо їх усунення та перешкоджання вчиненню кримінальних правопорушень. Профілактика поєднує низку заходів правового, соціального, технічного, організаційного та інформаційного характеру.

6. Під час розслідування шахрайства в інтернет-комерції можна проводити такі тактичні операції: «Фальшивий сайт», «Незаконна транзакція», «Встановлення IP-адреси», «Ідентифікація особи у віртуальному просторі», «Встановлення умислу», «Організація затримання шахрая, який діяв в мережі інтернет» та ін. В рамках вказаних 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.

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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анапольська А. І. Розслідування шахрайств і пов'язаних із ним злочинів, вчинених у сфері функціонування електронних розрахунків: автореф. дис. ... канд. юрид. наук : 12.00.09 / А.І. Анапольська; Харк. нац. ун-т внутр. справ. Харків, 2010. 20 с.

2. Андронік О. Л., Воронін А. В. Можливості та загрози електронної комерції в Україні. *Економіка і організація управління.* № 4 (44). 2021. С. 118-130.

3. Ансельмо Э. Киберпространство в международном законодательстве: опровергает ли развитие Интернета принцип территориальности в международном праве. *Экономические стратегии*. 2006. № 2. С. 24-31.

4. Антонюк І.А. Особливості допиту в кримінальних провадженнях щодо шахрайства у сфері надання послуг із посередництва у працевлаштуванні. *Науково-практичний господарсько-правовий журнал Підприємництво, господарство і право.*2020. № 9 (295). 260 с. С. 219–223.

5. Антонюк И.А. Особенности первоначального этапа расследования мошенничества в сфере предоставления посреднических услуг по трудоустройству. *Visegrad journal on human rights*. 2019. № 6-2. P. 21–26. (Словацкая Республика)

6. Аріт К. В. Особливості проведення слідчих (розшукових) дій під час розслідування злочинів у сфері економічної діяльності. *Право і Безпека.* 2013. № 2. С. 106–112.

7. Афанасенко С. І. Віктимологічна профілактика шахрайства: автореф. дис. ... канд. юрид. наук : 12.00.08 / Нац. акад. внутр. справ. Київ, 2013. 18 с.

8. Баганець О. Доказування причин та умов, що сприяли вчиненню кримінального правопорушення. *Юридична Україна*. 2013. № 8. С. 83–87.

9. Бакаянова Н. М., Кубаєнко А. В., Свида О. Г. Організація діяльності Національної поліції України та оперативних підрозділів: навчально-методичний посібник (для здобувачів вищої освіти денної форми

навчання) Одеса : Фенікс, 2020. 251 с. URL: http://dspace.onua.edu.ua/ (дата звернення 21.08.2020 р.).

10. Барицька Л. Включення України в інтеграційні процеси міжнародної електронної торгівлі. *Економіст.* 2002. № 9. С. 24 – 27.

11. Бевз С. І. Адміністративно-правове регулювання державного управління у сфері господарської діяльності в Україні: дис. док-ра юрид. наук / 12.00.07. Національний авіаційний університет. Київ, 2020. 26 с.

12. Березняк В. С., Павлова Н. В., Чаплинський К. О. Концептуальні засади методики розслідування кримінальних правопорушень у сфері нерухомості: теорія та практика: монографія / Київ. Одеса: Видавничий дім «Гельветика», 2022. 352с.

13. Бєгалов Є. П. Розслідування незаконного переправлення осіб через державний кордон України: дис. … докт. філ.: 081. Київ, 2020. 278 с.

14. Бєлік І. Б. Правове регулювання оподаткування електронної комерції : автореф. дис. ... канд. юрид. наук : 12.00.07 / І. Б. Бєлік ; Міжрегіон. акад. упр. персоналом. Київ, 2013. 18 с.

15. Біленчук П. Д., Лисиченко В. К., Клименко Н. І. та ін. Криміналістика: підручник / за ред. П. Д. Біленчука, 2-ге вид., випр. і доп. Київ: Атіка, 2001. 544 с

16. Біленчук П.Д., Біленчук Д.П., Міщенко В.Б., Мотлях О.І. Національна безпека України: сучасні інформаційні технології і можливі джерела безпеки. *Вісник Академії праці і соціальних відносин ФП України.* 1998. № 1. С. 61 – 72.

17. Білоус В.В. Проблеми методики розслідування фіктивного підприємництва: дис. ... канд. юрид. наук: 12.00.09 / Національна юридична академія імені Ярослава Мудрого. Харків., 2004. 179 с.

18. Білоусов Ю. В., Черняк О. Ю. Цивільно-правовий статус споживача: у контексті адаптації національного законодавства до законодавства Європейського Союзу: монографія. Київ: Науково-дослідний інститут приватного права і підприємництва НАПрН України. 2010. С. 190.

19. Блажівська Н. Є. Електронний правочин у цивільному праві України. дис. канд. юрид. наук / 12.00.03. Інститут законодавства Верховної Ради України. Київ, 2020. 246 с.

20. Вавриш А.В. Запобігання злочинам проти власності у сфері будівництва: Дис… канд. юрид. наук: 12.00.08 // НАВСУ. Київ., 2018. 275 с.

21. Веліканов С. В. Класифікація слідчих ситуацій у криміналістичній методиці: автореф. дис. … на здобуття наук. ступеня канд. юрид. Наук : 12.00.09 / Нац. юрид. акад. України. Харків, 2002. 22 с.

22. Венгерова Ю.В. Оцінка первісної інформації на початковому етапі розслідування злочинів, пов'язаних із туристичною діяльністю. *Актуальні проблеми експертного забезпечення досудового розслідування*: матер.наук.-практ. семінару (м. Дніпро, 29 трав. 2020 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. 372 с. С. 193–195.

23. Венгерова Ю.В. Проблемні аспекти організаційно-тактичного забезпечення допиту при розслідуванні злочинів у сфері туристичної діяльності. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*: Науковий журнал. 2020. № 3 (106). 328 с. С. 251–256.

24. Види оплат в інтернет-торгівлі. URL: https://medoc.ua/. (дата звернення 09.09.2019 р.).

25. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.]; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

26. Вимоги до продавців у сфері електронної комерції. URL: https://ips.ligazakon.net/ (дата звернення 09.12.2020 р.).

27. Вінник О. М. Правовий режим інтернет-магазина. *IUS PRIVATUM*. № 1. 2019. С. 5-14.

28. Волобуєв А. Ф. Загальні положення криміналістичної методики: лекція. Харків: Ун-т внутр. справ, 1996. 36 с.

29. Волобуєв А. Ф. Проблемні питання початку досудового розслідування. *Актуальні проблеми кримінального права, процесу та криміналістики*: матер. V міжнар. наук.-практ. конфер., присвяченої XX-річчю Національної академії правових наук України, 01 листоп. 2013 р., м. Одеса. Одеса: «Фенікс», 2013. С. 237–240.

30. Волобуєв А.Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва: автореф. дис... д-ра юрид. наук: 12.00.09 / Нац. юрид. акад. України ім. Я.Мудрого. Харків, 2001. 42 с.

31. Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва: дис. на здоб. наук. ст. д.ю.н. за спец. 12.00.09. Національний університет внутрішніх справ. Харків, 2001. 446 с.

32. Воронов І. О. Феномен BOTNET – латентна мобілізація сегментів мережі Інтернет для вчинення злочинів у сфері високих інформаційних технологій. *Вісн. Луган. держ. ун-ту внутрішніх справ*. Луганськ, 2010. № 3. С. 275-287.

33. Вплив війни на інтернет-торгівлю: як змінювалися онлайн-продажі рітейлерів протягом І півріччя 2022 року Джерело: URL: https://rau.ua/novyni/vpliv-vijni-na-internet/(дата звернення 22.11.22 р.).

34. Глинська Н. В., Лобойко Л. М., Марочкін О. І. Концептуальні основи побудови сучасного кримінального процесу України [текст] / та ін. : монографія: за заг. ред. О. Г. Шило. Харків: НДІ ВПЗ імені акад. В. В. Сташиса НАПрНУ, 2016. 264 с.

35. Глібко В.М. Роль документів у розслідуванні злочинів. *Теорія і практика правознавства*. Вип. 1 (9) / 2016. С.

36. Гнатенко В. С. Доказування обставин кримінальногоправопорушення слідчим. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО».*Випуск 32, 2021. С. 61-67.

37. Головкін Б. М. Види злочинності. Журнал східноєвропейського права. 2015. No. 18. С. 14 – 21. URL: http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf (дата звернення: 11.11.2020).

38. Голубєв В. О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітар. ун-т «ЗІДМУ», 2003. 296 с.

39. Даньшин М. В., Обаль О. О. Взаємодія слідчого з оперативними підрозділами під час проведення негласних слідчих (розшукових) дій у кримінальних провадженнях щодо економічних злочинів. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2019 № 38. С. 172-175.

40. Демідова В. В. Типові слідчі ситуації в методиці розслідування жорстокого поводження з тваринами. *Підприємство, господарство і право*. № 6/2019. С. 301-305.

41. Дехтярьов Є. В.Особливості розслідування шахрайств, вчинених у сфері виконання господарсько-договірних зобов'язань: автореф. дис. ... канд. юрид. наук : 12.00.09 / Акад. адвокатури України. Київ, 2011. 19 с.

42. Дехтярьов Є.В. Особливості тактики допиту особи, яка підозрюється у вчиненні шахрайства у сфері господарськодоговірних зобов’язань. Вісник Луганського державного університету внутрішніх справ імені Е.О, Дідоренка №3. 2011. С. 286-292.

43. Джужа О. М. Кримінологія: навч. посіб / О. М. Джужа, Ю. Ф. Іванов. Київ : Паливода А. В., 2008. 292 с.

44. Довженко О. Ю. Основи методики розслідування кіберзлочинів: автореф. дис. ... канд. юрид. наук (д-ра філософії) : 12.00.09 / МВС України, Харк. нац. ун-т внутр. справ. Харків, 2020. 20 с.

45. Доліновський Ю., Гула Л. Організація планування розслідування злочинів, що вчиняються під час публічних закупівель у сфері охорони здоров’я. 2018. URL:

https://science.lpnu.ua/sites/default/files/journal-paper/2019/aug/17951/19.pdf (дата звернення 02.07.2020 р.).

46. Дрозд В. Г. Запровадження міжнародно-правових стандартів захисту прав людини у світлі реформування кримінального процесуального законодавства. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 4 (80). С. 58–68.

47. Дубинський А. Я., Шостак Ю. І. Організація і діяльність слідчо-оперативної групи. Київ: КВШ, 1981. 49 с.

48. Дуда Х. І. Поняття комп'ютерних слідів злочину. *Науковий вісник Національного університету біоресурсів і природокористування України.* 2014. Вип. 197. Ч. 1. С. 262-267.

49. Дунаєвська Л. Г., Маркевич Я. С. Слідчі ситуації, що виникають при розслідуванні медичних злочинів. *Науковий вісник Ужгородського національного університету,* 2015. С. 126-128.

50. Дутов М. М. Правове забезпечення розвитку електронної комерції : автореф. дис. … канд. юрид. наук: 12.00.04 / Інститут економіко-правових досліджень НАН України. Донецьк, 2003. 17 с

51. Електронна комерція – історія розвитку, визначення, плюси, мінуси і перспективи.
URL:http://radka.in.ua/poradi/elektronnakomerciia-istoriia-rozvit.html (дата звернення 12.08.2019 р.).

52. Еннан Р. Правовідносини у сфері електронної комерції: досвід Європейського союзу. *Юридичний вісник*. 2019. № 1. С. 87-92.

53. Еннан Руслан Євгенович. Правове регулювання відносин у мережі Інтернет. URL: http://aphd.ua/publication-173/ (дата звернннення 22.09.2019).

54. Єфімов М. М., Павлова Н. В., Чучко С. В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу Інтернет: теоретичні та праксеологічні засади: монографія. Вид-во Гельветка, 2022. 202 с.

55. Єфімов М.М. Криміналістичний аналіз окремих сучасних видів шахрайства: проблемні питання. *Науковий вісник публічного та приватного права*. Випуск 5, том 1, 2021. С. 116-121.

56. Єфімов М.М. Теоретичні та практичні засади методики розслідування кримінальних правопорушень проти моральності. дис. … докт. юрид. наук.12.00.09. Дніпропетровський державний університет внутрішніх справ, Дніпро, 2021. 514 с.

57. Желіховський В. М. Правові засади електронної комерції в Україні : автореф. дис. ... канд. юрид. наук : 12.00.07 / Київ. нац. ун-т внутр. справ. Київ, 2007. 20 с.

58. Жерж Н.А., Дирдін М.Є. Слідчі ситуації та типові криміналістичні версії щодо особи злочинця при розслідуванні окремих насильницьких злочинів. *Науковий вісник Ужгородського національного університету*, 2015. С. 117-121.

59. Журавель В. А. Криміналістичні методики: сучасні наукові концепції: монографія. Харків: Апостиль, 2012. С. 202.

60. Журавель В.А. Система слідчих дій та тактичні операції в структурі окремої криміналістичної методики розслідування злочинів // Вісник Академії правових наук України. 2009. № 2 (57). С. 197 – 202.

61. Закон України «Про електронну комерцію» (із змінами і доповненнями, внесеними Законом України від 23 березня 2017 року N 1977-VII). URL :http://search.ligazakon.ua/l_doc2.nsf/link1/T150675.html. (дата звернення 12.08.2019 р.).

62. Запорожець Р. А. Запобігання шахрайству у сфері іпотечного кредитування: дис. … канд. юрид. наук (доктора філософії) за спеціальністю 12.00.08. Національна академія внутрішніх справ, Київ, 2017. 288 с.

63. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою: дис. канд. юрид. наук (12.00.09). ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом, Київ, 2021. 246 с.

64. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою:автореф. дис. на здобуття наук. ступеня канд. юрид. наук / 12.00.09. ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», Київ, 2021. 20 с.

65. Захарова Г. В. Організація і тактика проведення окремих слідчих (розшукових) дій при розслідуванні шахрайства у сфері туризму, вчиненого організованою групою. *Науковий вісник публічного та приватного права*. 2019. Вип. 2. Т. 3. С. 209–214.

66. Заяць К. Д. Методика розслідування шахрайств: дис. ... канд. юрид. наук: 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2020. 196 с.

67. Калініна І. В. Ситуаційна обумовленість розслідування господарських злочинів, пов'язаних із підробленням документів. *Ученые записки Таврического национального университета им. В.И. Вернадского.* 2013. Том 26(65). С. 212–217.

68. Капцош В.Я. Стан та особливості розвитку Інтернет-торгівлі товарами в міжнародному вимірі. *Науковий вісник Ужгородського національного університету*. № 13 (1). 2017. С. 115-119.

69. Качковський М. С. Типові слідчі ситуації початкового етапу розслідування умисного введення в обіг на ринку України небезпечної продукції. URL: http://www.pravoznavec.com.ua/period/article/40748/%CA (дата звернення: 03.09.2021).

70. Кириленко Н.Ю. Методика розслідування шахрайств у сфері побутових відносин: автореф. дис. ... канд. юрид. наук : 12.00.09 / Нац. Ун-т «Одеська юридична академія». Одеса., 2013. 20 с.

71. Кирилюк О. Ю. Договори, що укладаються з використанням електронних засобів зв'язку: автореф. дис. ... канд. юрид. наук: 12.00.03 / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2015. 20 с.

72. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки

України. URL: https://essuir.sumdu.edu.ua/bitstreamdownload/123456789/73900/1/Kuzmenko_1414.pdf;jsessionid=0D53722C6B7AE27B50991265CECB5E63 (дата звернення 17.03.19 р.).

73. Кіберполіція викрила псевдоперевізника, який ошукав маріупольців. URL: https://cyberpolice.gov.ua/ (дата звернення 29.04.22 р.).

74. Кіберполіція викрила шахрая, який налагодив схему здачі в оренду неіснуючого житла вимушеним переселенцям. URL: https://cyberpolice.gov.ua/ (дата звернення 22.11.22 р.).

75. Кіберполіція Дніпропетровщини викрила зловмисників у привласненні понад 1,5 млн гривень на продажі неіснуючих товарів. URL: https://cyberpolice.gov.ua/ (дата звернення 05.12.22 р.).

76. Кіберполіція Івано-Франківщини викрила зловмисника у шахрайстві під виглядом продажу талонів на пальне. URL: https://cyberpolice.gov.ua/ (дата звернення 22.11.22 р.).

77. Коваль А. А. Забезпечення прав людини при провадженні негласних слідчих (розшукових) дій: монографія. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2019. 264 с.

78. Коваль М., Коваль І. Типові слідчі ситуації при розслідуванні терористичних актів із використанням вибухових пристроїв. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. № 2 (30), 2021. С. 184-192.

79. Ковальчук О. В., Пряхін Є. В. Методика розслідування шахрайства, пов’язаного з діяльністю кредитної спілки: монографія. Львів: ЛьвДУВС, 2021. 204 с.

80. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського Національного Університету*, 2021. С. 220-224.

81. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки: дис. док-ра філософії (за спеціальністю 081 – Право). Національна академія внутрішніх справ, Київ, 2021. 255 с.

82. Коршун О. В. Теоретичні та праксеологічні засади методики розслідування кримінальних правопорушень у сфері нерухомості: дис. канд. юрид. наук (док-ра філософії).081 – Право. ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом, Київ, 2021. 242 с.

83. Коршун О. В. Теоретичні та праксеологічні засади методики розслідування кримінальних правопорушень у сфері нерухомості: автореф. дис… на здобуття наук. ступеня канд. юрид. 12.00.09. ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», Київ, 2021. 20 с.

84. Костова Н. І. Правое регулювання відносин міжнародної електронної комерції. *Науковий вісник Ужгородського національного університету*, 2019. Серія ПРАВО. Випуск 54. Том 1. С. 73-75.

85. Кофанов А. В. Криміналістика: питання і відповіді: навч. посіб. для студ. ВНЗ. НАВС. Київ: ЦУЛ. 2011. 276 с.

86. Краус К. М., Краус Н. М., Манжура О. В. Електронна комерція та Інтернет-торгівля: навчально-методичний посібник. Київ. Аграр Медіа Груп, 2021. 454 с.

87. Кривенка О.І. «Оперативно-розшукова протидія шахрайствам через мережу Інтернет» : автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09 «Кримінальний процес, криміналістика, судово-медична експертиза, оперативно-розшукова діяльність». Харків, 2018. 20 с.

88. Кривопуск О. Г. Способи вчинення злісного невиконання обов’язків по по догляду за дитиною або за особою, щодо якої встановлена опіка чи піклування. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 3. С. 369-376.

89. Криміналістика / В. В. Пясковській, Ю. М. Чорноус, А. В. Іщенко, О. О. Апєксєєв та ін. Київ: Центр учбової літератури, 2015. 544 с

90. Криміналістика: [навч. посіб.] / Р. І. Благута, Р. І. Сибірна, В. М. Бараняк та ін. ; за заг. ред. Є. В. Пряхіна. Київ: Атіка, 2012. 496 с.

91. Криміналістика: навчальний посібник / за заг. ред. Є.В. Пряхіна. Львів: ЛьвДУВС, 2010. 540 с.

92. Криміналістика: підруч. для студ. юрид. спец. вищ. закл. освіти / за ред. В. Ю. Шепітька. 3-тє вид., переробл. і допов. Київ: Вид. Дім «Ін Юре», 2004. 736 с.

93. Криміналістика: підручник: у 2 т. Т. 1.; за ред. В. Ю. Шепітька. Харків: Право, 2019. 456 с.

94. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI: URL: http://www.rada.gov.ua/ (дата звернення 08.01.2021).

95. Кузьменко С.С. Розслідування шахрайства, пов'язаного з інвестуванням коштів у будівництво об'єктів нерухомості: дис. ... канд. юрид. наук. 12.00.09. Дніпр. Держ. ун-т. внутр. справ. Дніпро, 2019. 224 с.

96. Куратченко М. В. Особливості взаємодії слідчих та оперативних підрозділів при розслідуванні сутенерства та втягнення особи в заняття проституцією / М. В. Куратченко // Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 2. - С. 235-242.

97. Курман О.В. Методика розслідування шахрайства з фінансовіми ресурсами: дис... канд. юрид. наук: 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2002. 218 с.

98. Латиш К.В. Тактичні операції діагностичного рівня під час розслідування вандалізму. *Науковий вісник Ужгородського національного університету, Серія ПРАВО. Випуск 40*. Том 2. 2016. С. 114-117.

99. Лисенко В. В., Лисенко О. В. Негласні слідчі (розшукові) дій у розшуковій роботі слідчого. *Сучасні тенденції розвитку криміналістики та кримінального процесу*. Харків, 2017. С. 118-120.

100. Лихолоб В. Г. Віктимологія. Юридична енциклопедія. В 6 т. Т. 1: А-Г / редкол.: Ю. С. Шемшученко [та ін.]. Київ: Укр. енцикл., 1998. С. 472–473.

101. Логінова В.В. Поняття та значення слідчих ситуацій у методиці розслідування злочинів. *Форум права*. 2010. № 3. С. 278–283. URL: http://www.nbuv.gov.ua/e-journals/FP/2010- 3/10lvvmrz.pdf (дата звернення 21.09.2019 р.).

102. Лук‘янчиков Є. Д. Правове регулювання перевірки інформації про кримінальні правопорушення. *Теоретичні аспекти організації досудового розслідування*: матеріали всеукраїнської науковопрактичної конференції (м. Харків, 4 грудня 2015 р.). Харків : ХНУВС, 2015. С. 57-61.

103. Лук’янчиков Є. Д. Щодо поняття криміналістичної характеристики злочинів. *Історико-правовий часопис.* 2013. № 2. С. 107–113.

104. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. *Юридичний науковий електронний журнал*. 2014. № 4. С. 202–205.

105. Максимус Д. О., Юхно О. О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій: навч. посіб. / Д. О. Максимус, О. О. Юхно. Харків: НікаНова, 2013. 102 с.

106. Матусовский Г. А. Проблемы развития криминалистической профилактики. *Актуальні проблеми криміналістики*: Матеріали міжнар. наук.-практ. конф. (Харків, 25-26 вересня 2003 р.) / Редкол.: М. І. Панов (голов. ред.), В. Ю. Шепітько, В. О. Коновалова та ін. Харків, 2003. С. 38-41.

107. Матусовский Г. А., Сущенко В. Н. Организация работы аппаратов предварительного следствия органов внутренних дел. Харьков: Юрид. ин-т, 1983. 84 с.

108. Мацишин В. С. Особливості розслідування фальшивомонетництва: дис... канд. юрид. наук. 12.00.09. Національна академія внутрішніх справ України. Київ, 2002. 298 с.

109. Михеенко М.М. Доказывание в советском уголовном судопроизводстве. Київ: Изд-во при Киевском университете издательского объеденения «Вища школа», 1984. 134 с.

110. Мізерак А. Б. Шахрайство при інтернет-торгівлі: схеми та аспекти запобігання. Маркетинг і контролінг: сучасні виклики підприємництв, Київ, 2017 р. 153-155.

111. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: дис… канд. юрид. наук: 12.00.09 / Академія праці і соціальних відносин Федерації профспілок України. Київ, 2005. 221 с.

112. Мудряк Т. О. Криміналістичні проблеми розслідування шахрайства з фінансовими ресурсами та шляхи їх вирішення. *Порівняльно-аналітичне право*. 2014. № 1. С. 279–281.

113. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах: монографія / за ред. проф. В. Ю. Шепітька. Харків: Право, 2009. 168 с.

114. На Миколаївщині слідчі та кіберполіцейські викрили шахрая на продажу неіснуючих товарів. URL: https://cyberpolice.gov.ua/ (дата звернення 02.12.22 р.).

115. Найпопулрніші способи шахрайства в електронній комерції. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-samye-populyarnye-sposoby-moshennichestva-v-elektronnoj-kommercii (дата звернення 12.10.2020р.).

116. Науково-практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М. І. Хавронюка. - 10-те вид., переробл. та допов. Київ : ВД «Дакор», 2018. 1360 с. С. 564.

117. Науково-практичний коментар Кримінального кодексу України / За ред. М.І. Мельника, М.І. Хавронюка. Київ: Каннон, А.С.К., 2002. 1104 с.

118. Одарченко А. М., Сподар К. В. Особливості електронної комерції та перспективи її розвитку в Україні. *Бізнесінформ.* №1. 2015. С. 342-346.

119. Одерій А.В, Шульга А.О. Основи методики розслідування вбивств на замовлення та вбивств, учинених під час здійснення релігійних ритуалів. Монографія. Донецьк: Донецький юридичний інститут. 2011. 326 с.

120. Одерій О. В. Предмет посягання як елемент криміналістичної характеристики злочинів проти довкілля: окремі аспекти. *Ученные записки Таврического национального университета им. В. И. Вернадского. Серия «Юридические науки».* 2013. Т. 26 (65). № 1. С. 255–259.

121. Олішевський О. В. Організація розслідування злочинів в органах внутрішніх справ (криміналістичний аспект): монографія / за заг. ред. О. М. Литвинова. Харків: Кримінологічна асоціація України; ФОП Ніконова, 2011. 200 с.

122. Олішевський О. В. Принципи організації розслідування злочинів. *Вісник Кримінологічної асоціації України*. № 3, 2013. С. 226-232.

123. Ортинський В. Особливості планування розслідування злочинів у сфері економіки. *Вісник Національного університету «Львівська політехніка». Юридичні науки.* 2017. № 861. С. 4-10.

124. Ошукали військових та волонтерів: кіберполіція Миколаївщини викрила зловмисників. URL: https://cyberpolice.gov.ua/ (дата звернення 05.12.22 р.).

125. Павлик М. П. Розслідування злочинів у сфері надання послуг із працевлаштування за кордоном: дис. … док-ра філософії (081 – Право). Національна академія внутрішніх справ, Київ, 2021. 247 с.

126. Павлова Н. В., Птушкін Д. А., Чаплинський К. О. Теоретичні засади методики розслідування шахрайства, пов’язаного з відчуженням об’єктів нерухомого майна громадян: монографія: монографія. Дніпр. державний університет внутрішніх справ. Херсон : Видавничий дім «Гельветика», 2019. 196 с.

127. Павлова Н. В., Рец В. В. Визначеннямісця та часу вчиненняшахрайства на первинному ринку нерухомості. *Науковий вісник Дніпропетровського університету внутрішніх справ.* № 3 (66). 2018. С. 139-143.

128. Павлова Н. В. Розслідування шахрайства при укладанні цивільноправових угод щодо відчуження житла: монографія. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ, 2008. 176 с.

129. Павлова Н.В. Предмет злочинного посягання у провадженнях щодо шахрайства. *Scientific journal The scientific heritage.* № 76 (76). Vol. 2. 2021. (Budapest, Hungary). С. 55-59.

130. Павлова Н.В. Щодо важливості дотримання прав і свобод особи під час проведення обшуку при розслідуванні кримінальних правопорушень, вчинених шляхом шахрайства.*Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. № 1. С. 190-196.

131. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: дис... канд. юрид. наук: 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2007. 211 с.

132. Паламарчук Л. П. Розслідування злочинів у сфері використання комп'ютерних технологій. Монографія. Київ:, 2007. 144 с

133. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж:автореф. дис. … канд. юрид. наук: 12.00.09 / Академія прокуратури. Київ, 2005. 21 с.

134. Підпалий В. В., Кислий А. М. Типові слідчі ситуації розслідування крадіжок в умовах великого міста. *Юридична наука*. № 2(104)/2020. С. 403-410.

135. Плетенець В.М. Криміналістичне забезпечення подолання протидії досудовому розслідуванню. дис. … док-ра юрид. наук. 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 494.

136. Поліцейські викрили в онлайн шахрайстві злочинну організацію, члени якої підозрюються у нанесенні потерпілим мільйонних збитків. URL: https://cyberpolice.gov.ua/ (дата звернення 01.12.22 р.).

137. Поляк Ю. П. Застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій та використання його результатів під час досудового розслідування: дис. … док-ра філософії (081 –

Право). Львівський державний університет внутрішніх справ, Львів, 2022. 230 с.

138. Порядок ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події: затв. наказом МВС України від 08.02.2019 № 100. URL: https://zakon.rada.gov.ua/laws/main/index (дата звернення 07.07.2020 р.).

139. Постанова Верховного Суду України від 24 листопада 2016 року: URL: http://www.shatarska.in.ua. (дата звернення 07.07.2020 р.).

140. Правила продажу товарів на замовлення та поза торговельними або офісними приміщеннями: затв. наказом Міністерства економіки України від 19.04.2007 № 103: http://zakon. rada.gov.ua/laws/show/z1181-07.

141. Правові засади електронної комерції в Україні. URL: http://eworks.com.ua/work/4073_Pravovi_zasadi_elektronnoi_komercii_v Ykraini. (дата звернення 12.08.2019 р.).

142. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII.URL: zakon2.rada.gov.ua/laws/show /675-19 (дата звернення 14.10.20 р.).

143. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: наказ МВС України № 575 від 07.07.2017 р. URL: https://zakon.rada.gov.ua/laws/main/index(дата звернення 22.11.20 р.).

144. Про затвердження Положення про Департамент протидії наркозлочинності НП України: Наказ НП України від 17.11.2015 р. № 95 / Офіційний матеріал Департаменту Документального забезпечення НП України.

145. Пропонував евакуацію з окупованих територій України: київські правоохоронці та кіберполіцейські викрили шахрая. URL: https://cyberpolice.gov.ua/ (дата звернення 05.12.22 р.).

146. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. Київ: Скіф, 2012. 728 с.

147. Пряхін Є. В. Криміналістичні засоби та методи розслідування кримінальних правопорушень: навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 164 с.

148. Птушкін Д.А. Розслідування шахрайства, вчиненого щодо об'єктів нерухомого майна громадян: дис. ... канд. юрид. наук: 12.00.09 / МВС України, Дніпр. держ. ун-т. внутр. справ. Дніпро, 2018. 240 с.

149. Пчеліна О. В. Особливості предмета доказування у кримінальних справах про економічні злочини та їх вплив на методику розслідування: автореф. дис. ... канд. юрид. наук : 12.00.09 / Харк. нац. ун-т внутр. справ. Х., 2010. 20 с.

150. Рєзнікова В. Поняття, значення та перспективи правового забезпечення електронної комерції в Україні. *Теорія і практика інтелектуальної власності*. 2015. № 2. С. 58–72.

151. Романенко Т. В. Особливості слідової картини шахрайств, що вчиняються в меружі Інтернет. *Молодий вчений*. № 1 (28). Частина. 2016 р. С. 51-54.

152. Ромців О. Планування як важливий напрям організації розслідування злочинів у сфері службової діяльності в умовах протидії. 2019. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2019/nov/19983/romciv.pdf (дата звернення 08.08.2021 р.).

153. Сазонов М. М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения. *Виктимология.* 2018. № 2 (16). С. 55–60.

154. Самойленко О. А. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник. Одеса, 2020. 112 с.

155. Самойленко О. А. До питання оцінки слідчим матеріалів первинної перевірки оперативної інформації про злочин, вчинений у кіберпросторі. *Науковий юридичний журнал.* № 7. 2019. С. 145-151.

156. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: автореф. дис. ... канд. юрид. наук: 12.00.09. Донецьк, 2014. 18 с.

157. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: дис. … канд. юрид. наук: 12.00.09. Донецьк, 2014. 226 с

158. Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки. *Проблеми правознавства та правоохоронної діяльності.* 2014. № 4. С. 25–31. URL: http://nbuv.gov.ua/UJRN/pppd_2014_4_6 (дата звернення 12.09.2019 р.).

159. Сафронов С. О. Методика розслідування умисного заподіяння тяжкого і середньої тяжкості тілесних ушкоджень: дис. ... канд. юрид. наук: 12.00.09. Харків: Університет внутрішніх справ МВС України, 1999. 229 с.

160. Скакун В. Криптовалюта в нерухомості. 29 жовтня 2019. URL: https://dom.ria.com/uk/articles/kriptovalyuta-v-nedvizhimosti-247565.html. (дата звернення 09.09.2019 р.).

161. Слідчі (розшукові) дії: навч. посібник / О. В. Авраменко, Р. І. Благута, Ю. В. Гуцуляк та ін.; за заг. ред. Р. І. Благути та Є. В. Пряхіна. Львів: ЛьвДУВС, 2013. 416 с.

162. Смаглюк О.В. Шахрайство за кримінальним кодексом України 2001 року: дис... канд. юрид. наук: 12.00.08 / Національна академія внутрішніх справ України. К., 2003. 179 с.

163. Справа № 202/1574/19: Ухвала Іменем України від 10 квітня 2019 року м. Дніпро Слідчого судді Індустріального районного суду м.

Дніпропетровська. URL: https://youcontrol.com.ua/statcatalog/ img/logo.svg. (дата звернення 20 грудня 2020).

164. Справа № 757/14259/19-к: Ухвала іменем України від 20 березня 2019 року слідчого судді Печерського районного суду м. Києва: URL: https://youcontrol.com.ua/. (дата звернення 01.09.2019 р.).

165. Справа № 757/36594/19-к. Ухвала іменем України. 15 липня 2019 року слідчий суддя Печерського районного суду м. Києва. URL: https://zakononline.com.ua/ldb/assets/images/nonoptimised/svg/mobile-logo.svg (дата звернення 20.12.19 р.).

166. Справа № 405/5286/20. Архів Ленінського районного суд м. Кіровограда, 2021 р.

167. Старенький О.С. Щодо визначення поняття меж доказування у кримінальному провадженні. *Часопис Національного університету «Острозька академія». Серія «Право*». 2014. №1(9).

168. Старушкевич А. В. Криміналістична характеристика злочинів: навч. посіб. Київ: НВТ «Правник» НАВСУ, 1997. 41 с.

169. Степанюк Р. Л. Тактичні завдання розслідування злочинів, вчинених у бюджетній сфері України. *Вісник Харківського національного університету внутрішніх справ.* 2012. № 1. С. 141–146.

170. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика та удосконалення системи криміналістичної техніки в Україні. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2022. Вип. 3 (99). С. 283-294.

171. Степанюк Р.Л. Проблеми формування криміналістичної характеристики окремих видів і груп злочинів. *Вісник Кримінологічної асоціації України*. 2013. № 5. С. 173-180.

172. Степанюк Р.Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека.* 2013. № 3. С. 110–115.

173. Степанюк Р.Л. Типові тактичні операції в методиці розслідування злочинів, вчинених у бюджетній сфері. *Право і Безпека*. 2012. № 1. С. 204-208.

174. Стецюк М. М Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача.*Використання досягнень сучасної науки й техніки в розкритті злочинів*: матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лют. 2021 р.) / Київ: Нац. акад. внутр. справ, 2021. С. 55-58.

175. Стрільців О. М., Крижна В. В., Максименко О. В. та ін. Особливості розслідування кримінальних правопорушень, пов’язаних із розповсюдженням у мережі Інтернет забороненого контенту: метод. рек. / за заг. ред. Ю. Ю. Орлова. Київ: Нац. акад. внутр. справ, 2014. 80 с.

176. Тарасова О.В. Удосконалення законодавства щодо кримінальної відповідальності за шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 3 ст. 190 Кримінального Кодексу України) Актуальні проблеми держави і права. 2014. Вип. 72. С. 481-488.

177. Тардаскіна Т.М. Електронна комерція: навчальний посібник / Тардаскіна Т.М., Стрельчук Є.М., Терешко Ю.В. Одеса: ОНАЗ ім. О.С. Попова, 2011. С. 33

178. Татаров О.Ю. Фаринник В. І. Початок досудового розслідування за кримінальним процесуальним кодексом України: доповідь. Новації кримінально-процесуального законодавства. Дніпропетровськ, 2012. URL: http://www.dduvs.in.ua/assets/files/ news3/KPK/material.doc

179. Тертичний Я. С. Детермінанти розвитку електронної комерції в умовах глобальної дигіталізації: дис. канд. екон. наук: 08.00.02. Донецький національний університет імені Василя Стуса, Вінниця, 2021. 20 с.

180. Типології легалізації (відмивання) доходів, одержаних злочинним шляхом, через ринок нерухомого майна: Наказ Державний комітет

фінансового моніторингу України №265 від 19.12.2008: URL: http://uapravo.net/index.htm (дата звернення 04.09.2018 р.).

181. Тіщенкова С.О. Теоретико-прикладні засади організації та планування у розслідуванні кримінальних правопорушень. матеріали Міжнародної науково-практичної конференції «Міжнародна та національна безпека: теоретичні та прикладні аспекти (тенденції, проблеми та шляхи їх вирішення» (17березня 2023 року). м. Дніпро. Дніпропетровський державний університет внутрішніх справ, 2023.

182. Товкун Л.В., Перепелиця М.О. Правове регулювання електронної комерції та особливості її оподаткування в Україні та світі. *Юридичний науковий електронний журнал*. № 3/2022. С. 178-182.

183. Томин С. В. Обєкт та предмет профілактики кримінальних правопорушень як окремого вчення криміналістики. *Прикарпатський юридичний вісник*. Випуск 3(12), 2016. С. 123-127.

184. У Дніпрі кіберполіція викрила зловмисників у шахрайстві з використанням фішингу на платформі оголошень. URL: https://cyberpolice.gov.ua/ (дата звернення 22.11.22 р.).

185. У Києві суд призначив покарання чоловіку за продаж неіснуючого військового спорядження. URL: https://cyberpolice.gov.ua/ (дата звернення 22.11.22 р.).

186. Українці стали удвічі частіше стикатися з інтернет-шахраями. URL: https://biz.nv.ua/ukr (дата звернення 12.10.2020р.).

187. Участь спеціаліста-криміналіста під час проведення окремих слідчих (розшукових) дій: Навчальний посібник [Є.Ю. Свобода, А.В. Кофанов, А.В. Самодін та ін.] Вінниця: ТОВ «Нілан-ЛТД», 2018. 432 с.

188. Федишин І. Б. Електронний бізнес та електронна комерція (опорний конспект лекцій для студентів напрямку «Менеджмент» усіх форм навчання) / Тернопіль: ТНТУ імені Івана Пулюя, 2016. 97 с.

189. Фридман И.Я. Вопросы профилактики преступлений при криминалистическом исследовании документов. Київ. : КНИИСЭ, 1968. 88 с.

190. Хань Г. А. Теоретичні засади планування та організації розслідування злочинів: дис. … канд. юрид. наук: 12.00.09. Донецьк, 2007. 221 с.

191. Хараберюш О. І. Інформаційно-телекомунікаційні технології у протидії контрабанді. *Право і суспільство*. - 2014. - № 2. - С. 217-221

192. Харківські кіберполіцейські спільно з правоохоронцями Німеччини викрили одного з організаторів транснаціональної шахрайської групи: збитки понад 600 тис євро. URL: https://cyberpolice.gov.ua/ (дата звернення 21.09.22 р.).

193. Хитра А. Я. Взаємодія слідчого та органу дізнання при провадженні кримінальних справ : курс лекцій / А. Я. Хитра, В. О. Кучер. Львів : Держ. ун-т внутрішніх справ, 2009. 100 с.

194. Царьов Р. Ю. Електронна комерція: навчальний посібник з підготовки бакалаврів. Одеса: ОНАЗ ім. О. С. Попова, 2010. 112 с.

195. Чайковська В. П. Електронна комерція в Україні: сучасний стан та тенденції розвитку. *Національна економіка. Інтелект ХХ*І. № 3. 2016. С. 38-48.

196. Чаплинський К.О. Організація і тактика слідчих дій при розслідуванні злочинів, учинених організованими злочинним угрупуваннями: монограф. Дніпро: Юрид. акад. М-ва внутр. справ, 2004. 192 с.

197. Чаплинський К.О. Тактичне забезпечення проведення слідчих дій: монограф. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2010. 560 с.

198. Чередник К. О. Розслідування шахрайства на ринку нерухомості, вчиненого злочинними угрупованнями: дис. … канд. юрид. наук. 12.00.09. Відкритий міжнародний університет розвитку людини «Україна», Київ, 2019. 260 с.

199. Черненко О. О. Роль слідчих підрозділів ОВС України у профілактиці злочинності (історичний досвід). *Інформація і право*. № 1(16)/2016. С. 180-187.

200. Чернишов Г.М. Фінансове шахрайство в інвестиційно-будівельній сфері: кримінологічне дослідження: дис. ... канд. юрид. наук: 12.00.08. Одеса, 2016. 255 с.

201. Чернявський С. С. Методика розслідування злочинів у сфері банківського кредитування: автореф. дис... канд. юрид. наук: 12.00.09 /; Національна академія внутрішніх справ України. Київ, 2002.

202. Черняк О. Ю. Цивільно-правовий статус споживача у контексті адаптації національного законодавства до законодавства Європейського Союзу: автореф. дис. … на здобуття наук. ступеня канд. юрид. наук: 12.00.03. Науково-дослідний інститут приватного права іпідприємництва НАПрН України. Київ, 2011. 22 с.

203. Чорний А. М. Тактичні операції при розслідуванні умисних вбивств. *Правоісуспільство*. № 2. 2011. С. 238-242.

204. Чучко С. В.Оцінка первісної інформації та коло обставин, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет: окремі аспекти.*Наук. вісн. Дніпроп. держ. ун-ту внутр. справ.* № 3. 2020. С. 304–310.

205. Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет: дис. док-ра філософії. 081 – Право. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 276 с.

206. Чучко С.В. Способи вчинення шахрайства, пов’язаного із придбанням товарів через мережу Інтернет. VisegradJournalonHumanRights. 2019. № 6. С. 234-238.

207. Чучковська А. В. Правове регулювання господарських договорів, що вчиняються через мережі електрозв’язку : автореф. дис. … канд. юрид. наук : 12.00.03 / КНУ ім. Тараса Шевченка. Київ, 2004. 20 с.

208. Шалева О. І. Електронна комерція. Навч. посіб. Київ: Центр учбової літератури, 2011. 216 с

209. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*: наук.-практ. журнал. Київ: МНДЦ при РНБО України. 2014. № 1 (32). С. 213-225.

210. Шапочка С.В. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет. *Правова інформатика*. № 3(43)/2014. С. 89-95.

211. Шапочка С.В. Інформаційна безпека та кібершахрайство: матеріали міжнар. наук.- практ. конф. *Внутрішні та зовнішні загрози національній безпеці держави*, (Київ, 2 квітня 2013 р.); НАВС. К. : ТОВ "Три К", 2013. С. 188-191.

212. Шахрайства в Інтернеті в умовах війни. URL: https://it-kharkiv.com/ (дата звернення 12.10.2022р.).

213. Шевчук В. М. Значення тактичних завдань для побудови та реалізації типових тактичних операцій у кримінальному провадженні. *Национальный юридический журнал: теория и практика.* 2016. Octombrie. С. 204–207.

214. Шевчук В. М. Значення теоретичних завдань для формування тактичних операцій. *Юридична наука*. 2014. № 3. С. 7–16.

215. Шкригун Ю.О. «Електронний бізнес», «електронна комерція» та «електронна торгівля»: відмінності й особливості. *Управління економікою: теорія та практика: Зб. наук. праць.* Київ: ІЕП НАНУ, 2020. С. 312-325.

216. Шуляк Ю.Л. Кримінальна відповідальність за шахрайство: порівняльно-правове дослідження: автореф. дис. ... канд. юрид. наук : 12.00.08 / Шуляк Ю. Л. ; Нац. акад. внутр. справ. Київ, 2011. 20 с.

217. Юдін О. М., Макарова М. В., Лавренюк Р. М. Системи електронної комерції: створення, просунення і розвиток: монографія. Полтава: РВВ ПУЕТ, 2011. 201 с.

218. Янковий М. О. Криміналістична профілактика злочинів як складова слідчої діяльності. *Актуальні проблеми держави і права*. 2008. С. 55-59.

219. Яровенко Г.М., Сковронська А.І., Бояджян М.М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка*. 2018. № 7. URL: http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf

220. Яровенко Г. М. Моделювання портретів потенційних шахрая та жертви банківських шахрайств [Електронний ресурс] / Г. М. Яровенко, В. О. Ковач. // Ефективна економіка. - 2018. - № 10.

221. Яцишин М. М. Актуальні завдання профілактики злочинів з боку засуджених в установах виконання покарань. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/2027/1/actual.pdf (дата звернення 11.09.2019 р.).

222. 60 шахраїв у сфері електронної комерціалізації затримані під час міжнародної операції. URL: https://www.europol.europa.eu/ (дата звернення 21.02.2020 р.).

223. Javed A. R., Ahmed W., Alazab M., Jalil Z., Kifayat K., Gadekallu T. R. A compre hensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. IEEE Access. 2022. Vol. 10. P. 110650–11089. DOI: 10.1109/ACCESS.2022. 3142508.

224. KuznichenkoY, DykhaMV, PavlovaN, FrolovS, HryhorashO. Defining the probability of bank debtors' default using financial solvency assessment models. *Banks and Bank Systems.* 13 (2), 1-11. DOI: 10.21511/bbs.13(2).2018.01.

225. Merchant Fraud Journal: eCommerce Fraud News Publication. URL: https://www.merchantfraudjournal.com/top-ecommerce-fraud-protection-solutions/ (дата звернення: 29.11.2021).

226. Merchant Fraud Journal: eCommerce Fraud News Publication. URL: https://www.merchantfraudjournal.com/top-ecommerce-fraud-protection-solutions/ (дата звернення: 29.11.2021).

227. Merchant Fraud Journal: eCommerce Fraud News Publication. URL: https://www.merchantfraudjournal.com/top-ecommerce-fraud-protection-solutions/ (дата звернення: 29.11.2021).

228. Qijun Gu, Peng Liu Denial of Service Attacks. Qijun Gu, Peng Liu. URL: https://s2.ist.psu.edu/paper/DDoS-Chap-GuJune-07.pdf (датазвернення 17.03.19 р.).

229. Reznik O., Fomenko A., Melnychenko A., Pavlova N., Prozorov A. Features of the initial stage of investigating fraud with financial resources in cyberspace. Amazonia Investiga. 2021. Vol. 10 (Issue 41). May. P. 141–150.

230. RyanC. HybridRisk: Thetruthbehindfirstpartyfraud. Chris Ryan // The official site of the company "Experian". 2015. URL:http://www.experian.com/blogs/insights/2015/10/hybrid-risk-thetruth-behind-first-party-fraud/. (дата звернення 12.10.2020р.).

231. ShapochkaS. PreventingFraudUsingComputerNetworks / SerhiyVladimirovichShapochka. InternalSecurity. 2013. № 2. P. 63-75.

232. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998. United Nations publication. URL: https://www. uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf. (дата звернення 12.08.2019 р.).

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані 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.

Додаток Б

Зведені результати

анкетування 179 працівників оперативних підрозділів, 186 слідчих, 80 дізнавачів, 89 працівників органів прокуратури України та 113 обізнаних осіб

	З а п и т а н н я	
1	**Ваш вік:**	
	20-25 років	**20**
	25-30 років	**31**
	31-40 років	**41**
	41 рік і старше	**8**
2	**Який досвід практичної роботи:**	
	до 1 року	**8**
	від 1 до 3 років	**21**
	від 3 до 5 років	**19**
	від 5 до 10 років	**23**
	більше 10 років	**29**
3	**Яку посаду займаєте:**	
	слідчий	**14**
	старший слідчий	**38**
	працівник експертної установи	**9**
	керівник слідчого підрозділу	**6**
	працівник оперативного підрозділу	**13**
	процесуальний керівник (прокурор прокуратури)	**8**
	інше	**12**
4	**Ваша освіта:**	
	тільки вища юридична	**86**
	вища юридична та інша за іншим профілем	**45**
	вища освіта за іншим профілем	**9**
	середня освіта	**2**
5	**Чи можете Ви надати інформацію щодо розслідування шахрайства в інтернет-комерції:**	
	Так	**100**

	Ні	**0**
6	**На Вашу думку, що найчастіше стає предметом злочинного посягання:**	
	послуги	**56**
	гроші	**34**
	товари побутового прзначення	**12**
	товари військового призначення	**9**
	медикаменти	**16**
	криптоалюта	**4**
	Інше	**12**
7	**Чи вважаєте Ви, що розслідування шахрайства в інтернет-комерції потребує кваліфікації слідчого у цьому напряму:**	
	так	**98**
	ні	**2**
8	**Яким чином Ви підвищуєте свою кваліфікацію:**	
	шляхом спілкування з фахівцями у сфері інтернет-комерції, (консультування)	**72**
	шляхом вивчення спеціальної літератури	**71**
	не підвищую, оскільки не маю часу	**12**
	проходження спеціальних курсів	**5**
	інше	**17**
9	**Чи є необхідність у використанні спеціальних знань при розслідуванні шахрайства в інтернет-комерції:**	
	так	**100**
	ні	**0**
10	**Чи вважаєте Ви, що питання, які стосуються інтернет-комерції, є достатньо складними для сприйняття слідчим без належної підготовки та консультацій:**	
	так	**94**
	ні	**6**
11	**Між якими органами (установами) здебільшого здійснюється взаємодія при розслідуванні шахрайства в інтернет-комерції:**	
	між слідчим та оперативним працівником	**100**

	між слідчим та представникам державних та приватних установ, які мають відношення до інтернет-комерції	**94**
	між слідчим та банківським установами	**9**
	необхідно міжнародне співробітництво	**13**
	інше	**34**
12	**Взаємодія між слідчим та оперативними підрозділами у справах щодо шахрайства в інтернет-комерції, має місце у вигляді:**	
	взаємний обмін інформацією та спільний її аналіз	**95**
	спільне планування слідчих (розшукових) дій та оперативно-розшукових заходів	**93**
	надання допомоги при виконанні заходів забезпечення кримінального провадження (привід, затримання тощо)	**54**
	інше	**34**
13	**Вкажіть, які слідчі (розшукові) та процесуальні дії у провадженнях даної категорії звичайно проводяться:**	
	огляд місця події	**93**
	допит	**100**
	обшук	**76**
	пред’явлення для впізнання	**31**
	слідчий експеримент	**8**
	призначення експертиз	**100**
	освідування	**8**
	тимчасовий доступ до речей та документів	**100**
	інші	**53**
14	**Участь спеціаліста в проведенні слідчих дій (інших процесуальних дій) у провадженнях даної категорії найбільш поширена при проведенні:**	
	обшуків	**41**
	тимчасового доступу до речей та документів	**38**
	допиту	**14**
	огляду документів	**71**
	відібрання зразків підпису та почерку для почеркознавчого дослідження	**31**
	призначення експертиз	**100**

	інше	**38**
15	**Як Ви вважаєте, які можуть бути основні причини великої тривалості розслідування шахрайства в інтернет-комерції:**	
	складність розмежування злочину від цивільно-правового делікту	**84**
	недостатність кваліфікації у слідчого в галузі інтернет-комерції	**35**
	відсутність технічного оснащення	**21**
	інше	**34**
16	**Чи потребувалась додаткова консультація фахівця перед призначенням експертиз:**	
	так, у частині підготовки порівняльного матеріалу та у частині поставлених питань	**86**
	ні	**14**
17	**Вкажіть основні тактичні помилки, яких припускаються слідчі, які розслідують данікримінальні правопорушення:**	
	неправильно підібраний або неповний тактичний комплекс дій	**76**
	порушення процесуального порядку проведення слідчих (розшукових) дій	**83**
	проведення деяких процесуальних дій без участі спеціаліста	**56**
	«поверхневий» характер процесуальних дій, ігнорування встановлення низки важливих обставин	**85**
	обрання неправильної послідовності процесуальних дій, зокрема тактичних операцій	**61**
	інше	**38**
18	**Як Ви відноситесь до проведення тактичних операцій при розслідуванні шахрайства в інтернет-комерції:**	
	позитивно	**98**
	не розумію необхідності	**2**
19	**Які тактичні операції Ви вважаєте найбільш ефективними при розслідуванні шахрайства в інтернет-комерції:**	
	спрямованих на встановлення ознак організованості	**91**
	спрямованих на встановлення співучасників	**93**
	спрямованих на подолання протидії	**88**
	спрямованих на встановлення місця знаходження особи-власника нерухомості, який тримається у неволі	**37**

	інші	**54**
20	**Чи вважаєте Ви планування у справах даної категорії обов'язковим:**	
	так	**98**
	ні	**2**
21	**Що є основними причинами рідкого застосування пред'явлення для впізнання у режимі відеоконференції**	
	складність підготовки й проведення впізнання в режимі відеоконференції	**37**
	відсутність необхідного технічного забезпечення слідчого підрозділу ГУНПУкраїни	**62**
22	**Як Ви вважаєте, чи є поширеними факти вчинення протидії розслідуванню кримінальним правопорушенням даної категорії:**	
	так	**94**
	ні	**6**

Додаток В

Результати вивчення
192 кримінальних проваджень з проблематики дослідження (Вінницька, Дніпропетровська, Запорізька, Івано-Франківська, Київська, Львівська, Миколаївська, Одеська, Черкаська та Чернівецька області, м. Київ)

	Досліджувані питання	
1	**Предметом посягання у кримінальних провадженнях щодо шахрайства в інтернет-комерціївиступали:**	
	гроші	**56**
	майно	**12**
	цінні папери	**9**
	криптовалюта	**4**
	інше	**34**
2	**Слідову картинушахрайства в інтернет-комерції складають:**	
	печатки й штампи	**72**
	засоби маскування	**36**
	сліди рук	**90**
	інформація в телефоні	**64**
	дані електронної переписки	**59**
	інше	**34**
3	**Місцем вчинення шахрайства в інтернет-комерції:**	
	банківські установи	**65**
	місце знаходження сервера	**97**
	інше	**16**
4	**Способи вчинення шахрайства в інтернет-комерції включали:**	
	підготовка, безпосереднє вчинення, приховування	**100**
	безпосереднє вчинення, приховування	
	тільки вчинення	
5	**Відомості про особу шахрая:**	
	1) освіта: середня-спеціальна вища загальна середня освіта	 **11** **73** **16**
	2) місце проживання: сільська місцевість	 **12**

	велике місто	**88**
	3) вік: від 18 до 25 років від 25 до 45років від 40 до 50 років після 50 років.	 **11** **66** **12** **11**
	4) сімейний стан: є сім'я немає сім'ї	 **66** **44**
	5) наявність судимості: є судимість немає судимості	 **19** **81**
	6) склад осіб: вчинено однією особою вчинено двома особами вчинено злочинним угрупованням	 **4** **23** **73**
	7) стать: жіноча чоловіча	 **21** **79**
6	**Відомості про потерпілого:**	
	1) освіта: середня вища неповна середня освіта	 **31** **49** **20**
	2) чи належить потерпілий до соціально незахищених верств населення: так ні	 **25** **75**
	3) стать: чоловік жінка	 **43** **57**
	4) рівень матеріального благополуччя: заможні особи особи низького рівня достатку	 **35** **65**
7	**Наявність у кримінальному провадженні плану розслідування:**	
	план є	**95**
	плану немає	**5**
	На початковому етапі розслідування висуваються версії	

8	**щодо:**	
	події	**97**
	епізодів злочинної діяльності	**93**
	способу вчинення шахрайства	**99**
	осіб, які володіють інформацією про шахрайство	**95**
	злочинців, їх кількості, місцезнаходження та ролі кожного у вчиненні шахрайства	**95**
	інше	**55**
9	**Найбільш поширені типові слідчі ситуації:**	
	злочинець відомий, є достатні фактичні дані, що свідчать про конкретні обставини кримінального правопорушення та його причетність до нього	**24**
	виявлено факт здійснення шахрайства, злочинець відомий, але доказів для повідомлення про підозру недостатньо	**21**
	злочинець відомий, наявні матеріальні сліди злочину й очевидці злочинної події, але він переховується від слідства й суду	**24**
	злочинець невідомий, відсутні матеріальні сліди та очевидці злочину	**10**
	інше	**21**
10	**Які слідчі (розшукові), процесуальні дії проводились у справах щодо шахрайства в інтернет-комерції:**	
	допит	**100**
	одночасний допит двох або більше осіб	**59**
	обшук	**73**
	огляд місця події	**97**
	огляд предметів та документів	**99**
	пред’явлення для впізнання осіб	**28**
	пред’явлення для впізнання предметів та документів	**19**
	призначення експертиз	**100**
	тимчасовий доступ до речей та документів	**85**
	інше	**56**
11	**При розслідуванні шахрайства в інтернет-комерції виникає необхідність у вилученні таких об’єктів:**	
	документи, що підтверджують виконання договірних зобов’язань	**67**
	розрахунково-платіжні відомості	**64**
	банківські платіжні документи	**55**
	флеш-носії	**36**
	комп’ютерна техніка й програмне забезпечення	**31**
	інше	**34**
	Свідками у справах щодо шахрайства в інтернет-комерції,	

12	**виступали:**	
	знайомі та родичі потерпілого	**76**
	знайомі та родичі підозрюваного	**29**
	особи, які випадково стали свідками події (знаходилися у банківській установі, чули розмову між шахраєм та потерпілим)	**47**
	інтернет-провайдери	**31**
	інші	**44**
13	**Одночасний допит проводився:**	
	між підозрюваними особами	**55**
	між підозрюваним та потерпілим	**69**
	між підозрюваним та свідками	**11**
	між свідками	**8**
14	**До обшуку залучались:**	
	спеціалісти-криміналісти	**44**
	спеціаліст у галузі комп'ютерних технологій	**56**
	спеціалісти з інших галузей	**31**
	інші	**34**
15	**Які технології захисту комп'ютерної інформації використовували злочинці:**	
	аутентифікація конкретного користувача	**22**
	криптографічний захист інформації	**12**
	засоби архівації на спеціалізованому сервері	**34**
	інше	**32**
16	**Які результати проведення обшуку:**	
	позитивні	**85**
	негативні	**15**
17	**Причини негативного результату обшуку:**	
	недостатня підготовка	**15**
	витік інформації про планування обшуку	**14**
	порушення процесуальних вимог	**22**
	втручання в процес проведення обшуку сторонніх осіб	**21**
	недотримання криміналістичних рекомендацій щодо правил проведення відео-, фотозйомки	**31**

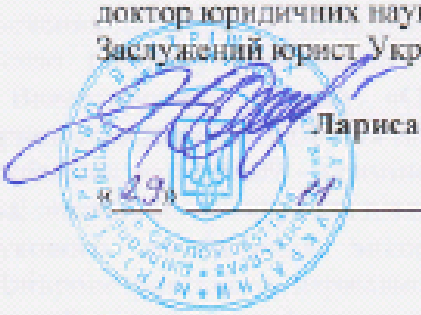
	відсутність спеціаліста (спеціалістів)	**8**
	інше	**34**
18	**Призначення експертиз:**	
	почеркознавчі	**69**
	технічні експертизи документів	**98**
	комп'ютерно-технічні	**11**
	трасологічні	**8**
	портретна	**9**
	експертиза відео звукозапису	**7**
	інші	**7**
19	**Об'єкти, які пред'являлися для впізнання при розслідуванні шахрайства в інтернет-комерції:**	
	особа	**44**
	предмети	**32**
	інше	**34**
20	**В якій формі чинилася протидія розслідуванню:**	
	застосування корупційних механізмів	**42**
	протидія у формі надання неправдивих свідчень	**71**
	приховування інформації	**54**
	фізичний та психологічний вплив на учасників кримінального процесу	**31**
	фальсифікація та знищення доказів	**62**
	інше	**41**
21	**Який комплекс дій та заходів, спрямованих на подолання протидії розслідуванню:**	
	пред'явлення для впізнання поза візуальним спостереженням	**36**
	проведення допитів у режимі відеоконференції	**11**
	проведення НСРД шляхом використання технічних засобів контролю, прослуховування телефонних та інших розмов, візуального спостереження, з метою отримання конфіденціальної інформації щодо діяльності ЗУ, намірів здійснення протидії у певній формі та відносно до певних суб'єктів	**37**
	здійснення заходів щодо реагування на виявлені прояви (обшуки, затримання)	**62**
	інше	**38**

Додаток Г

АКТИ ВПРОВАДЖЕННЯ

результатів дослідження у наукову діяльність, освітній процес та правохоронну практику

ЗАТВЕРДЖУЮ
Проректор
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор
Заслужений юрист України



Лариса НАЛИВАЙКО

«29» 11 2022 року

АКТ
впровадження у науково-дослідну діяльність
Дніпропетровського державного університету внутрішніх справ
результатів дисертаційного дослідження

29 листопада 2022 року м. Дніпро

Про впровадження у науково-дослідну діяльність Дніпропетровського державного університету внутрішніх справ основних результатів дисертаційного дослідження Рейнгольд Андрія Валентиновича «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голови: заступника директора Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Обшалова С.В.

членів комісії: завідувача кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Дарагана В.В.

професора кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, професора Пирога І.В.

професора кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Плетеня В.М.

відповідно до Пріоритетних напрямів наукових досліджень Дніпропетровського державного університету внутрішніх справ на 2020-2024

роки та загальноуніверситетської теми наукових досліджень «Актуальні проблеми кримінально-правового, кримінального процесуального та криміналістичного забезпечення протидії злочинності в Україні (державний реєстраційний номер 0118U100431) і напрямів досліджень наукової школи ДДУВС «Криміналістичне забезпечення досудового розслідування» склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження Рейнгольд Андрія Валентиновича на тему: «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Основні результати наукового дослідження використовуються у науково-дослідницькій роботі Дніпропетровського державного університету внутрішніх справ з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень, пов'язаних із шахрайствами.

Результати дисертації відображаються у наступних наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (статтях і тезах доповідей на конференціях і семінарах):

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).

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.

Наукові публікації відповідають планам науково-дослідних та дослідно-конструкторських робіт профільних кафедр Дніпропетровського державного університету внутрішніх справ на 2022-2023 навчальний рік.

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Дніпропетровського державного університету внутрішніх справ при проведенні наукових досліджень на замовлення Головного Управління Національної поліції в Дніпропетровській області.

Голова комісії: **Сергій ОБШАЛОВ**

Члени комісії: **Валерій ДАРАГАН**

Ігор ПИРІГ

Віктор ПЛЕТЕНЕЦЬ

ЗАТВЕРДЖУЮ
Директор
Навчально-наукового інституту права
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
доктор юридичних наук, професор

Анатолій КИСЛИЙ

«___» _____ 2022 року

АКТ
впровадження в освітній процес Навчально-наукового інституту права ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» результатів дисертаційного дослідження

24 листопада 2022 року м. Київ

Про впровадження в освітній процес і наукову діяльність ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» дисертаційного дослідження Рейнгольд Андрія Валентиновича «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Комісія у складі:

голова: завідувача кафедри правоохоронної та антикорупційної діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доктора юридичних наук, професора Заросила В.О.

членів комісії: заступника директора Навчально-наукового інституту права та ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», кандидата юридичних наук, доцента Тимошенка Ю.П.

професора кафедри правоохоронної та антикорупційної діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доктора юридичних наук, доцента Коваченка О.І.

відповідно до Положення про організацію освітнього процесу і наукової діяльності в ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія

управління персоналом» склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження Рейнгольд Андрія Валентиновича на тему: «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у вигляді наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

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).

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.

Наукове дослідження Рейнгольд Андрія Валентиновича на тему: «Основи методики розслідування шахрайства в інтернет-комерції» виконане відповідно до сучасних потреб правоохоронної практики та стану розвитку юридичної науки.

Члени комісії дійшли висновку, що надані здобувачем Науково-дослідного інституту публічного права Рейнгольд Андрієм Валентиновичем матеріали (наукові статті та тези доповідей) свідчать про належний науковий, методологічний та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, відображені у науково-методичних матеріалах навчальних дисциплін з кримінального права, кримінального процесу та криміналістики для здобувачів вищої освіти бакалавра і магістра, використовуються при підготовці методичних рекомендацій та в системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та можуть використовуватися в освітньому процесі та науковій діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» при підготовці здобувачів вищої освіти.

Голова комісії: **Володимир ЗАРОСИЛО**

Члени комісії: **Юрій ТИМОШЕНКО**

Олександр КОЗАЧЕНКО

ЗАТВЕРДЖУЮ
Проректор
Національної академії
внутрішніх справ
доктор юридичних наук, професор
заслужений діяч науки і техніки
полковник поліції

Сергій ЧЕРНЯВСЬКИЙ

«__» _____ 2022 року

АКТ
впровадження у науково-дослідну діяльність та освітній процес Національної академії внутрішніх справ результатів дисертаційного дослідження

Про впровадження у науково-дослідну діяльність та освітній процес Національної академії внутрішніх справ основних результатів дисертаційного дослідження Рейнгольд Андрія Валентиновича «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голови: заступника начальника навчально-методичного відділу Національної академії внутрішніх справ, кандидата юридичних наук, капітана поліції Бистрицького Б.Ю.

членів комісії: професора кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктора юридичних наук, професора, підполковника поліції Чорноус Ю.М.

професора кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидата юридичних наук, доцента, полковника поліції Пясковського В.В.

відповідно до Пріоритетних напрямів наукових досліджень Національної академії внутрішніх справ на 2022-2023 навчальний рік склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження Рейнгольд Андрія Валентиновича на тему: «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата

юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Основні результати наукового дослідження використовуються у науково-дослідницькій роботі Дніпропетровського державного університету внутрішніх справ з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень, пов'язаних із шахрайствами.

Результати дисертації відображаються у наступних наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (статтях і тезах доповідей на конференціях і семінарах):

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.

Рейнгольд А.В. Концептуальні підходи до побудови криміналістичної характеристики шахрайства в інтернет-комерції. *Юридична наука*. 2019. № 6. Том 2. С. 73–77.

Рейнгольд А.В. Оцінка первинної інформації на початку розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 1. Том 2. С. 114–118.

Рейнгольд А.В. Типові слідчі ситуації під час розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 2. Том 2. С. 129–133.

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.

Рейнгольд А.В. Стан розробленості проблеми боротьби із шахрайством в інтернет-комерції. *KELM*. 2022. № 7. С. 112–117 (Республіка Польща).

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.

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.

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.

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.

Наукові публікації відповідають планам науково-дослідних та дослідно-конструкторських робіт профільних кафедр Національної академії внутрішніх справ на 2022-2023 навчальний рік.

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Національної академії внутрішніх справ при проведенні наукових досліджень.

Заступник начальника навчально-методичного відділу
Національної академії внутрішніх справ
кандидат юридичних наук,
капітан поліції **Богдан БИСТРИЦЬКИЙ**

Професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ
доктор юридичних наук, професор
підполковник поліції **Юлія ЧОРНОУС**

Професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ
кандидат юридичних наук, доцент
полковник поліції **Валим ПЯСКОВСЬКИЙ**

ЗАТВЕРДЖУЮ
Заступник декана факультету № 1
з навчально-методичної роботи
Харківського національного
університету внутрішніх справ
доктор юридичних наук, доцент

Владислав НЕВЯДОВСЬКИЙ

«17» 11 2022 року

АКТ
впровадження у науково-дослідну діяльність та освітній процес Харківського національного університету внутрішніх справ результатів дисертаційного дослідження

Про впровадження у науково-дослідну діяльність та освітній процес Харківського національного університету внутрішніх справ основних результатів дисертаційного дослідження Рейнгольд Андрія Валентиновича «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голови: завідувач кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент Кікінчук В.В.

членів комісії: завідувач кафедри кримінального процесу та організації досудового слідства факультету № 1 Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент Романюк В.В.

професор кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор Степанюк Р.Л.

відповідно до Основних напрямів наукових досліджень Харківського національного університету внутрішніх справ на 2021-2024 роки склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження Рейнгольд Андрія Валентиновича на тему: «Основи методики

розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Основні результати наукового дослідження використовуються у науково-дослідницькій роботі Харківського національного університету внутрішніх справ з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень, пов'язаних із шахрайствами.

Результати дисертації відображаються у наступних наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (статтях і тезах доповідей на конференціях і семінарах):

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.

Рейнгольд А.В. Концептуальні підходи до побудови криміналістичної характеристики шахрайства в інтернет-комерції. *Юридична наука*. 2019. № 6. Том 2. С. 73–77.

Рейнгольд А.В. Оцінка первинної інформації на початку розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 1. Том 2. С. 114–118.

Рейнгольд А.В. Типові слідчі ситуації під час розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 2. Том 2. С. 129–133.

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.

Рейнгольд А.В. Стан розробленості проблеми боротьби із шахрайством в інтернет-комерції. *KELM*. 2022. № 7. С. 112–117 (Республіка Польща).

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.

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.

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.

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.

Наукові публікації відповідають планам науково-дослідних та дослідно-конструкторських робіт профільних кафедр Харківського національного університету внутрішніх справ на 2022-2023 навчальний рік.

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дисертаційного дослідження, грунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України. Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Харківського національного університету внутрішніх справ при проведенні наукових досліджень.

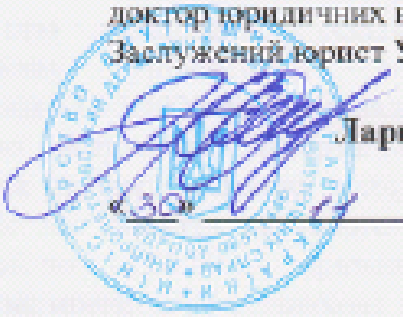
Голова комісії:
завідувач кафедри криміналістики
та судової експертології
Харківського національного
університету внутрішніх справ
кандидат юридичних наук, доцент **Василь КІКІНЧУК**

Члени комісії:
завідувач кафедри кримінального процесу
та організації досудового слідства
Харківського національного
університету внутрішніх справ
кандидат юридичних наук, доцент **Віталій РОМАНЮК**

професор кафедри криміналістики
та судової експертології
Харківського національного
університету внутрішніх справ
доктор юридичних наук, професор **Руслан СТЕПАНЮК**

ПІДПИС ЗАСВІДЧУЮ
Факультет №1 ХНУВС
28/12 «14» 11 2022 р.

ЗАТВЕРДЖУЮ
Проректор
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор
Заслужений юрист України



Лариса НАЛИВАЙКО

«30» _____ 2022 року

АКТ
впровадження в освітній процес
Дніпропетровського державного університету внутрішніх справ
результатів дисертаційного дослідження

30 листопада 2022 року м. Дніпро

Про впровадження в освітній процес Дніпропетровського державного університету внутрішніх справ основних результатів дисертаційного дослідження Рейнгольд Андрія Валентиновича «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Комісія у складі:

голови: начальниці навчально-методичного відділу Дніпропетровського державного університету внутрішніх справ, кандидата біологічних наук Кириченко С.В.

членів комісії: заступника директора Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Обшалова С.В.

завідувача кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, професора Чаплинського К.О.

завідувача кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Дарагана В.В.

завідувача кафедри кримінального процесу та стратегічних розслідувань Дніпропетровського державного університету внутрішніх справ, кандидата юридичних наук, доцента Санакоєва Д.Б.

відповідно до Положення про організацію освітнього процесу в Дніпропетровському державному університеті внутрішніх справ, затвердженого наказом ДДУВС від 13.05.2020 № 352 склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження Рейнгольд Андрія Валентиновича на тему: «Основи методики розслідування шахрайства в інтернет-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у вигляді наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

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).

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.

Члени комісії дійшли висновку, що надані матеріали (наукові статті та тези доповідей) свідчать про належний науковий, методологічний та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, відображені у науково-методичних матеріалах навчальних дисциплін з кримінального процесу, криміналістики та оперативно-розшукової діяльності для здобувачів вищої освіти бакалавра і магістра, використовуються при підготовці методичних рекомендацій та в системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та можуть використовуватися в освітньому процесі Дніпропетровського державного університету внутрішніх справ при підготовці здобувачів вищої освіти ННІ права та підготовки фахівців для підрозділів Національної поліції, факультету підготовки фахівців для підрозділів кримінальної поліції, факультету підготовки фахівців для підрозділів превентивної діяльності, студентів ННІ права та інноваційної освіти та навчально-наукового інституту заочного навчання та підвищення кваліфікації.

Голова комісії: **Світлана КИРИЧЕНКО**

Члени комісії: **Сергій ОБШАЛОВ**

Костянтин ЧАПЛИНСЬКИЙ

Валерій ДАРАГАН

Дмитро САНАКОЄВ

«ЗАТВЕРДЖУЮ»
Начальник
Головного управління
Національної поліції
в Дніпропетровській області
генерал поліції третього рангу
кандидат юридичних наук

Анатолій ЩАДИЛО
«__» _____ 2023 року

АКТ

впровадження в практичну діяльність органів досудового розслідування матеріалів дисертації Рейнгольд Андрія Валентиновича на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність на тему «Основи методики розслідування шахрайства в інтернет-комерції»

Комісія у складі: заступника начальника СУ ГУНП – начальника відділу розслідування злочинів, скоєних проти життя та здоров'я особи, кандидата юридичних наук Мельниченка А.В., заступника начальника відділу розслідування злочинів у сфері транспорту СУ ГУНП в Дніпропетровській області, кандидата юридичних наук Серединського В.В., заступника начальника відділу розслідування злочинів у сфері господарської та службової діяльності Швеня Я.Р., склала це акт про те, що матеріали дисертації здобувача Науково-дослідного інституту публічного права Рейнгольд Андрія Валентиновича на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність на тему «Основи методики розслідування шахрайства в інтернет-комерції» можуть застосовуватись у практичній діяльності слідчих підрозділів, а також під час проведення занять в системі службової підготовки.

Заступник начальника СУ ГУНП –
начальник відділу розслідування злочинів,
скоєних проти життя та здоров'я особи
кандидат юридичних наук **Андрій МЕЛЬНИЧЕНКО**

Заступник начальника відділу
розслідування злочинів у сфері транспорту
СУ ГУНП в Дніпропетровській області
кандидат юридичних наук **Валентин СЕРЕДИНСЬКИЙ**

Заступник начальника відділу
розслідування злочинів у сфері
господарської та службової діяльності **Ярослав ШВЕНЬ**