НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

УДК 343.98: 343.131

ПЕРХУН СЕРГІЙ ОЛЕКСАНДРОВИЧ

ДИСЕРТАЦІЯ

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ОСНОВИ ФОРМУВАННЯ МЕТОДИКИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ ІНТЕРНЕТ-БАНКІНГУ

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

_____С. О. Перхун

Науковий керівник –
Чорноус Юлія Миколаївна,
доктор юридичних наук,
професор

Київ – 2025

АНОТАЦІЯ

Перхун С. О. Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. – Науково-дослідний інститут публічного права; Дніпровський державний університет внутрішніх справ, Київ, 2025.

У дисертаційному дослідженні на монографічному рівні опрацьовано теоретичні та практичні засади методики розслідування шахрайства у сфері використання інтернет-банкінгу. Удосконалено систему складових методики розслідування досліджуваного виду протиправного діяння, у якій виокремлено такі елементи: криміналістична характеристика шахрайства; аналіз початкових відомостей та їхня оцінка; перелік обставин, що підлягають встановленню в кримінальному провадженні; типові слідчі ситуації, які формуються під час розслідування шахрайства, а також алгоритми їх реалізації; сукупність тактичних операцій для реалізації конкретних завдань розслідування; взаємодія уповноважених осіб з окремими підрозділами Національної поліції та іншими державними органами в кримінальному провадженні; профілактична діяльність уповноважених осіб у кримінальному провадженні; тактика проведення окремих СРД, НСРД та інших процесуальних дій на початковому етапі розслідування шахрайства у сфері використання інтернет-банкінгу; тактика проведення окремих СРД, НСРД та інших процесуальних дій на подальшому етапі розслідування; особливості використання спеціальних знань у кримінальному провадженні.

Удосконалено теоретичні концепції стосовно інформативного наповнення криміналістичної характеристики шахрайства у сфері

використання інтернет-банкінгу, у якій виокремлено такі елементи: спосіб підготовки, безпосереднього вчинення та приховування шахрайства; обстановка вчинення шахрайства у сфері використання інтернет-банкінгу; слідова картина протиправного діяння; особа шахрая; особа потерпілого.

Надано криміналістичне наповнення типових способів підготовки, безпосереднього вчинення та приховування шахрайства у сфері використання інтернет-банкінгу під час користування послугами в інтернет-магазинах, на різноманітних сайтах, зокрема фішинг, спамінг, кардінг

Встановлено сукупність інформаційних даних щодо обстановки вчинення шахрайства у сфері використання інтернет-банкінгу на основі опрацювання просторово-часових, економічних, психологічних і соціальних факторів.

Наведено перелік потенційних місць учинення протиправних діянь: місця розташування електронно-обчислювальної техніки, що були використані під час учинення кримінальних правопорушень (місце проживання підозрюваного, місця загального доступу); місця розміщення терміналів, банків, банкоматів та інших фінансових установ; місце перебування особи потерпілого, на яку були спрямовані шахрайські дії.

Акцентовано увагу на сукупності даних стосовно матеріальних та особистісних слідів, а також виокремлення серед них особливої групи слідів, характерних для вчинення шахрайства у сфері використання інтернет-банкінгу – цифрових (електронних, віртуальних) слідів, які здебільшого виявляють у таких місцях: профілях соціальних мереж (Facebook, Instagram, Twitter), месенджерах (Telegram, Viber), застосунках для переписок криптовалютного спрямування (Binance), кеш-пам’яті онлайн магазинів, базах інтернет-провайдерів тощо.

Окреслено криміналістично значущі ознаки *особи злочинця* (шахрая). Сформовано вірогідний «портрет» особи шахрая. Наголошено, що особам, які вчиняють шахрайства у сфері інтернет-банкінгу, притаманні високий рівень інтелекту й винахідливість.

Запропоновано структуру злочинної організації, що здійснює шахрайські дії у сфері використання інтернет-банкінгу, до якої входять такі групи осіб: 1) організатори; 2) адміністратори сайтів, де розміщують неправдиві відомості стосовно товарів або надання послуг; 3) продавці, які спілкуються з потенційними потерпілими (здебільшого через телефонні розмови або sms-переписки); 4) спамери (особи, які здійснюють розсилку листів стосовно інтернет-магазинів з продажу товарів або надання різноманітних послуг); 5) фішери (особи, які розсилають листи для отримання особистої інформації потенційних потерпілих); 6) програмісти (особи, які створюють спам-боти для розсилки та віруси для потенційних атак); 7) хакери (особи, які здійснюють вірусні атаки на об'єкти, що зацікавили злочинну організацію); 8) охоронці; 9) корумповані представники органів державної влади й управління, працівники правоохоронних органів, які беруть участь у прикритті організованої злочинної діяльності

Надано характеристику *особі потерпілого,* визначено й схарактеризовано віктимогенні групи потерпілих. Виокремлено віктимогенні групи осіб, стосовно яких було вчинено шахрайські дії.

Виокремлено особливості аналізу й оцінки первинної інформації, а також визначено коло обставин, що підлягають встановленню в кримінальному провадженні. Зокрема, встановлено, що первинна інформація, яка слугувала підставою для внесення відомостей до ЄРДР, була одержана уповноваженими особами з таких джерел: а) заяви, листи й повідомлення, що надійшли від потерпілих від шахрайських дій, – 67 %; б) заяви, листи й повідомлення від громадян, які стали свідками вчинення шахрайських дій або одержали про них інформацію, – 14 %; в) звернення, заяви, листи й повідомлення від працівників фінансових установ різних форм власності – 9 %; г) матеріали справ, які було виокремлено з інших кримінальних проваджень, – 3 %; д) матеріали, одержані в межах реалізації НСРД або розшукових заходів, – 7 %.

Окреслено сукупність обставин, що підлягають встановленню під час

розслідування шахрайства у сфері використання інтернет-банкінгу, а саме: 1) обставини, що розкривають умови та способи вчинення шахрайства (інформація про час і місце його вчинення, відомості щодо способу підготовки, безпосереднього вчинення та приховування шахрайських дій, зокрема застосування спам-ботів, використання вірусних програм до ЕОТ потерпілих, використання різноманітних шахрайських схем), засоби, що використовували під час учинення шахрайських дій; 2) обставини, що характеризують особу злочинця чи групу осіб (кількість шахраїв, схема розподілу між ними обов'язків, визначення їхньої ролі в злочинному угрупованні); 3) обставини, що характеризують особу потерпілого (віктимність її дій, базовий чи професійний користувач ЕОТ); 4) причинно-наслідкові зв'язки між діями шахраїв і результатами, що їх характеризують; 5) встановлення причин та умов, що сприяли вчиненню шахрайських дій; 6) обставини, що обтяжують або пом'якшують покарання; 7) вид і розмір шкоди, що завдана шахрайськими діями; 8) обставини, що є приводом для звільнення шахрая від кримінальної відповідальності.

Сформовано типові слідчі ситуації, що виникають під час розслідування шахрайства у сфері використання інтернет-банкінгу: вчинено шахрайські дії, наявна особистісна доказова база, злочинця (шахрая) встановлено – 27 %; здійснено шахрайські дії, є особистісна доказова база, злочинця (шахрая) не встановлено – 52 %; вчинено шахрайські дії, наявна особистісна та матеріальна доказова база, злочинця (шахрая) не встановлено – 16 %; вчинено шахрайські дії, повністю відсутня доказова база – 5 %. На основі узагальнення судово-слідчої практики запропоновано алгоритми вирішення наведених типових слідчих ситуацій, що виникають на початковому етапі розслідування.

Доведено, що вирішення слідчих ситуацій безпосередньо залежить від ефективної взаємодії слідчого з працівниками оперативних підрозділів Національної поліції, а також представниками органів державної влади та управління. Під час розслідування шахрайства у сфері використання

інтернет-банкінгу особливого значення набуває «обмін інформацією» як одна з найбільш ефективних форм взаємодії, особливо в умовах запровадженого воєнного стану.

Конкретизовано особливості організації і тактики проведення процесуальних дій на початковому етапі розслідування шахрайства у сфері використання інтернет-банкінгу. На початковому етапі розслідування слідчому необхідно провести такі заходи: допит потерпілого, огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета), огляд і долучення до справи фотографій або відеозаписів, розшук і встановлення особи шахрая, аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі), візуальне спостереження за особою, негласне зняття інформації з транспортних телекомунікаційних мереж, призначення експертизи тощо.

Запропоновано низку тактичних завдань, які уповноважені особи мають реалізувати в кримінальному провадженні, а також розроблено комплекси дій для їх вирішення в межах проведення початкового та подальшого етапів розслідування, зокрема: 1) тактичне завдання «Профілактика протиправних дій» – реалізація відповідних профілактичних заходів для усунення причин та умов учинення шахрайства у сфері використання інтернет-банкінгу; 2) тактичне завдання «Встановлення шахрая» – проведення низки процесуальних дій і заходів, спрямованих на виконання вказаного завдання; 3) тактичне завдання «Встановлення співучасників в організованій групі чи злочинній організації» – з'ясування ймовірної участі та ролі шахрая в злочинному угрупованні.

Розкрито організаційно-тактичне забезпечення проведення процесуальних дій на подальшому етапі розслідування шахрайства у сфері використання інтернет-банкінгу. З'ясовано, що на цьому етапі розслідування в 100 % випадків коло підозрюваних встановлено.

Наведено безконфліктні та конфліктні ситуації *допиту підозрюваного*. Для вирішення конфліктних ситуацій доцільно використовувати низку

тактичних прийомів допиту, серед яких ключове місце посідають встановлення психологічного контакту з підозрюваним, пред'явлення речових доказів (флеш-накопичувачі, скріншоти переписок із потерпілим, скріншоти із хмарних сховищ) і матеріалів кримінального провадження (протоколів допиту потерпілих та свідків, протоколів обшуку).

Запропоновано перелік питань, що необхідно з'ясувати під час допиту підозрюваного, а саме: 1) які способи застосовувалися для входу в застосунок інтернет-банкінгу (використання спам-ботів; реквізитів картки, одержаної від конкретного потерпілого шляхом шахрайських дій; використання реквізитів картки, отриманої з web-сторінок підставних інтернет-магазинів); 2) у який спосіб вчинено шахрайські дії (шляхом отримання доступу до ЕОТ з паролями, що встановив потерпілий; шляхом використання мережі Wi-Fi); 3) чи вчинено шахрайські дії організованою групою або злочинною організацією; якщо так, то якою є структура злочинного угруповання; 4) який статус та обов'язки кожного зі співучасників шахрайства; 5) яким чином розподілялися викрадені майно та грошові кошти між співучасниками; 6) протягом якого проміжку часу було вчинено шахрайські дії; 7) наявність учинення супутніх кримінальних правопорушень; 8) що за знаряддя й засоби використовувались під час учинення шахрайських дій (комп'ютери, смартфони, модеми, маршрутизатори, браузери, спам-боти); 9) якою є загальна сума грошових коштів була отримана шляхом реалізації шахрайських дій у сфері використання інтернет-банкінгу тощо.

Схарактеризовано організаційно-тактичне забезпечення проведення одночасного допиту двох або більше раніше допитаних осіб. Встановлено, що вказана процесуальна дія повинна бути спрямована на усунення невідповідностей у показаннях раніше допитаних осіб, зокрема: 1) підозрюваного та потерпілого (87 %) – як було вчинено шахрайські дії; які було застосовано засоби для їх учинення (комп'ютер, планшет, ноутбук, смартфон) тощо; 2) між підозрюваними (9 %) – які ролі в організованій групі чи злочинній організації вони виконували тощо; 3) підозрюваного та свідка

(2 %); 4) потерпілого та свідка (1 %); 5) між потерпілими (1 %).

Акцентовано увагу на обов'язковій реалізації пред'явлення підозрюваного для впізнання за фотографією та голосом. Надано перелік місць, де необхідно проводити обшук.

Визначено особливості використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу.

Серед основних форм використання спеціальних знань у кримінальному провадженні виокремлено такі: а) безпосереднє застосування уповноваженою особою спеціальних знань під час реалізації окремих слідчих (розшукових) дій, НСРД та інших процесуальних і розшукових заходів; б) залучення спеціаліста до проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій і розшукових заходів; в) консультативна допомога спеціаліста; г) призначення та проведення судових експертиз.

Надано пропозиції щодо внесення змін до ч. 1 ст. 71 КПК України, яку запропоновано викласти в такій редакції: «Спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками, що можуть бути застосовані під час досудового розслідування та судового розгляду шляхом надання довідок, пояснень, консультацій і висновків в усній чи письмовій формі для вирішення питань, що вимагають володіння відповідними спеціальними знаннями чи навичками».

На підставі узагальнення матеріалів кримінальних проваджень запропоновано обов'язкові судові експертизи, які необхідно призначати під час розслідування шахрайства у сфері використання інтернет-банкінгу, а саме: а) судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів, експертиза цифрової інформації, програмно-комп'ютерна експертиза); б) судово-бухгалтерська експертиза; в) інформаційно-комп'ютерна експертиза; г) експертиза телекомунікаційних систем і засобів.

Визначено окремі аспекти підготовки та проведення судових експертиз, а також об'єкти, які можуть бути направлені на експертизу.

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

– *законотворчій діяльності* – для вдосконалення законодавства у сфері використання банківських електронних платежів і запобігання кримінальним правопорушенням, пов'язаним із використанням інтернет-банкінгу, викладено низку практичних рекомендацій стосовно внесення змін і доповнень до чинного Кримінального процесуального кодексу України;

– *освітньому процесі* – під час викладання навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Кримінальний процес», «Криміналістика», «Оперативно-розшукова діяльність», а також підготовки підручників, навчальних посібників і монографічних досліджень (акт впровадження Національної академії внутрішніх справ від 19 квітня 2024 р.);

– *науковій діяльності* – для вдосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Національної академії внутрішніх справ від 27 травня 2024 р., Дніпровського державного університету внутрішніх справ від 30 травня 2024 р.);

– *правозастосовній діяльності* – для вдосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Управління стратегічних розслідувань в Дніпропетровській області ДСР Національної поліції України від 07 червня 2024 р., Головного слідчого управління Національної поліції України від 16 жовтня 2024 р.).

Ключові слова: шахрайство, інтернет-банкінг, досудове розслідування, банківські операції, електронний переказ, кіберзлочини, методика, криміналістична характеристика, профілактика, кримінальне правопорушення, типові слідчі ситуації, слідчі (розшукові) дії, негласні слідчі (розшукові) дії.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані
основні наукові результати дисертації:

1. Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

2. Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

3. Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).

4. Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

5. Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

6. Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

Наукові праці, що засвідчують апробацію матеріалів дисертації:

7. Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали

Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

8. Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200.

9. Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової системи України* : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123.

10. Перхун С. О. До питання визначення обставин, які підлягають встановленню під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення* : матеріали Міжнар. наук.-практ. конф. (Київ, 13–14 берез. 2023 р.). Київ : Наук.-дослід. ін-т публіч. права, 2023. С. 131–133.

SUMMARY

Perkhun S. O. Theoretical and practical foundations of the formation of fraud investigation methods in the field of Internet banking. – *Qualifying scientific work on manuscript rights.*

Dissertation for obtaining the scientific degree of candidate of legal sciences on the specialty 12.00.09 – criminal process and criminology; forensic examination; investigative activity. – Research Institute of Public Law; Dnipro State University of Internal Affairs, Kyiv, 2025.

In the dissertation research, the theoretical and practical principles of the

investigation method of investigating fraud in the field of Internet banking were worked out at the monographic level. The system of components of the methodology of the investigation of the investigated type of illegal act has been improved, in which the following elements are singled out: forensic characteristics of fraud; analysis of initial information and their evaluation; a list of circumstances to be established in criminal proceedings; typical investigative situations that arise during a fraud investigation, as well as algorithms for their implementation; a set of tactical operations for the implementation of specific investigative tasks; interaction of authorized persons with individual units of the National Police and other state bodies in criminal proceedings; preventive activity of authorized persons in criminal proceedings; the tactics of conducting individual SRD, NSRD and other procedural actions at the initial stage of fraud investigation in the field of Internet banking use; the tactics of conducting separate SRD, NSRD and other procedural actions at the subsequent stage of the investigation; peculiarities of the use of special knowledge in criminal proceedings.

The theoretical concepts related to the informative filling of the forensic characteristics of fraud in the field of Internet banking usage have been improved, in which the following elements are distinguished: the method of preparation, direct commission and concealment of fraud; the situation of committing fraud in the field of using Internet banking; trace picture of an illegal act; identity of the fraudster; the person of the victim.

A forensic analysis of typical methods of preparation, direct perpetration and concealment of fraud in the field of using Internet banking during the use of services in online stores, on various sites, including phishing, spamming, and carding, is provided.

A set of information data on the situation of committing fraud in the field of using Internet banking has been established based on the study of spatial-temporal, economic, psychological and social factors.

The list of potential places where illegal acts were committed is given: locations of electronic computing equipment that were used during the commission

of criminal offenses (place of residence of the suspect, places of public access); locations of terminals, banks, ATMs and other financial institutions; the place of residence of the victim, who was targeted by fraudulent actions.

Attention is focused on the set of data related to material and personal traces, as well as the identification among them of a special group of traces characteristic of committing fraud in the field of Internet banking - digital (electronic, virtual) traces, which are mostly found in the following places: social network profiles (Facebook, Instagram, Twitter), messengers (Telegram, Viber), cryptocurrency messaging applications (Binance), cache memory of online stores, databases of Internet providers, etc.

Criminologically significant features of the identity of a criminal (fraudster) are outlined. A probable "portrait" of the fraudster's person has been formed. It is emphasized that individuals who commit fraud in the field of Internet banking are characterized by a high level of intelligence and ingenuity.

The structure of a criminal organization that carries out fraudulent activities in the field of Internet banking is proposed, which includes the following groups of persons: 1) organizers; 2) administrators of sites that post false information about goods or services; 3) sellers who communicate with potential victims (mostly through phone calls or text messages); 4) spammers (persons who send letters regarding online stores selling goods or providing various services); 5) phishers (persons who send letters to obtain personal information of potential victims); 6) programmers (persons who create spam bots for distribution and viruses for potential attacks); 7) hackers (persons who carry out viral attacks on objects of interest to a criminal organization); 8) guards; 9) corrupt representatives of state authorities and management, employees of law enforcement agencies, who participate in the cover-up of organized criminal activity.

The character of the victim was given, and victimogenic groups of victims were defined and characterized. Victimogenic groups of persons against whom fraudulent actions were committed are singled out.

The specifics of the analysis and assessment of primary information are

highlighted, as well as the range of circumstances to be established in criminal proceedings. In particular, it was established that the primary information, which served as the basis for entering information into the EDPR, was obtained by authorized persons from the following sources: a) statements, letters and messages received from victims of fraudulent actions, – 67%; b) statements, letters and messages from citizens who witnessed the commission of fraudulent actions or received information about them – 14 %; c) appeals, statements, letters and messages from employees of financial institutions of various forms of ownership – 9 %; d) case materials that were separated from other criminal proceedings – 3 %; e) materials obtained within the scope of the implementation of NSRD or investigative measures – 7 %.

The totality of the circumstances to be established during the investigation of fraud in the field of internet banking use is outlined, namely: 1) circumstances that reveal the conditions and methods of committing fraud (information about the time and place of its commission, information about the method of preparation, direct commission and concealment of fraudulent actions, in particular the use of spam bots, the use of virus programs for the EOT of victims, the use of various fraudulent schemes), the means used in committing fraudulent acts; 2) circumstances that characterize the person of the criminal or a group of persons (the number of fraudsters, the scheme of distribution of duties between them, determination of their role in the criminal group); 3) circumstances characterizing the person of the victim (victim of her actions, basic or professional user of EOT); 4) cause-and-effect relationships between the actions of fraudsters and the results that characterize them; 5) establishing the reasons and conditions that contributed to the commission of fraudulent actions; 6) circumstances that aggravate or mitigate punishment; 7) type and amount of damage caused by fraudulent actions; 8) circumstances that are grounds for exempting the fraudster from criminal liability.

Typical investigative situations that arise during the investigation of fraud in the use of Internet banking have been formed: fraudulent actions have been

committed, the personal evidence base is available, the criminal (fraudster) has been identified – 27 %; fraudulent actions were carried out, there is a personal evidence base, the criminal (fraudster) has not been identified – 52 %; fraudulent actions were committed, there is a personal and material evidence base, the criminal (fraudster) has not been identified – 16 %; fraudulent actions were committed, there is a complete lack of evidence – 5 %. Based on the generalization of judicial and investigative practice, algorithms for solving the given typical investigative situations that arise at the initial stage of the investigation are proposed.

It has been proven that the resolution of investigative situations directly depends on the effective interaction of the investigator with the employees of the operational divisions of the National Police, as well as representatives of state authorities and management. During the investigation of fraud in the field of use of Internet banking, the «exchange of information» acquires special importance as one of the most effective forms of interaction, especially in the conditions of the introduced martial law.

The specifics of the organization and tactics of conducting procedural actions at the initial stage of the investigation of fraud in the field of Internet banking are specified. At the initial stage of the investigation, the investigator must conduct the following measures: interrogation of the victim, examination of the EOT of the victim (computer, smartphone, tablet), examination and attachment of photos or video recordings to the case, search and identification of the fraudster, audio control of the person by installing technical means in a publicly inaccessible place (vehicle, apartment), visual surveillance of the person, clandestine removal of information from transport telecommunication networks, appointment of expertise, etc.

A number of tactical tasks that authorized persons should implement in criminal proceedings have been proposed, as well as sets of actions have been developed to solve them within the framework of the initial and subsequent stages of the investigation, in particular: 1) tactical task «Prevention of illegal actions» –

implementation of appropriate preventive measures to eliminate the causes and conditions of committing fraud in the field of using Internet banking; 2) tactical task «Establishing a fraudster» – carrying out a number of procedural actions and measures aimed at fulfilling the specified task; 3) tactical task «Establishing co-conspirators in an organized group or criminal organization» – finding out the likely participation and role of a fraudster in a criminal group.

The organizational and tactical support for conducting procedural actions at the next stage of the investigation of fraud in the field of Internet banking use has been revealed. It was found that at this stage of the investigation, in 100 % of cases, the circle of suspects has been established.

Non-conflict and conflict situations of interrogation of the suspect are given. To resolve conflict situations, it is advisable to use a number of tactical interrogation techniques, among which the establishment of psychological contact with the suspect, the presentation of physical evidence (flash drives, screenshots of correspondence with the victim, screenshots from cloud storage) and criminal proceedings materials (interrogation protocols of victims and witnesses, search protocols) occupy a key place.

A list of questions that must be clarified during the questioning of the suspect is proposed, namely: 1) what methods were used to enter the Internet banking application (use of spambots; details of a card obtained from a specific victim through fraudulent actions; use of card details, obtained from the web pages of bogus online stores); 2) in what way fraudulent actions were committed (by gaining access to EOT with passwords set by the victim; by using a Wi-Fi network); 3) whether fraudulent actions were committed by an organized group or criminal organization; if so, what is the structure of the criminal group; 4) what is the status and duties of each of the accomplices of the fraud; 5) how the stolen property and funds were distributed among the co-conspirators; 6) during which period of time fraudulent actions were committed; 7) presence of related criminal offenses; 8) what tools and means were used when committing fraudulent actions (computers, smartphones, modems, routers, browsers, spam bots); 9) what is the

total amount of money received through the implementation of fraudulent actions in the field of using Internet banking, etc.

The organizational and tactical provision of simultaneous interrogation of two or more previously interrogated persons is characterized. It was established that the indicated procedural action should be aimed at eliminating inconsistencies in the testimony of previously interrogated persons, in particular: 1) the suspect and the victim (87 %) – how fraudulent actions were committed; which means were used for their implementation (computer, tablet, laptop, smartphone), etc.; 2) between suspects (9 %) – what roles they played in an organized group or criminal organization, etc.; 3) suspect and witness (2 %); 4) victim and witness (1 %); 5) between victims (1 %).

Attention is focused on the mandatory implementation of the presentation of the suspect for identification by photo and voice. A list of places where it is necessary to conduct a search is provided.

The peculiarities of the use of special knowledge during the investigation of fraud in the use of Internet banking have been determined.

Among the main forms of using special knowledge in criminal proceedings, the following are distinguished: a) direct use of special knowledge by an authorized person during the implementation of individual investigative (search) actions, NSRD and other procedural and search measures; b) involvement of a specialist in carrying out separate investigative (search) actions, NSRD and other procedural actions and search measures; c) advisory assistance of a specialist; d) appointing and conducting forensic examinations.

Proposals for amendments to Part 1 of Art. 71 of the Criminal Procedure Code of Ukraine, which is proposed to be presented in the following version: «A specialist in criminal proceedings is a person who possesses special knowledge and skills that can be applied during pre-trial investigation and court proceedings by providing certificates, explanations, consultations and conclusions in oral or written form to resolve issues that require the possession of relevant special knowledge or skills».

On the basis of summarizing the materials of criminal proceedings, mandatory forensic examinations are proposed, which must be appointed during the investigation of fraud in the use of Internet banking, namely: a) forensic examination of computer equipment and software products (examination of technical computer means, examination of digital information, software and computer examination); b) forensic accounting examination; c) information and computer expertise; d) examination of telecommunication systems and means.

Certain aspects of preparing and conducting forensic examinations, as well as objects that can be sent for examination, are defined.

The practical significance of the obtained results is that the theoretical propositions, conclusions and practical recommendations presented and argued in the dissertation are implemented and used in:

– *legislative activity* – in order to improve the legislation in the field of using bank electronic payments and prevent criminal offenses related to the use of Internet banking, a number of practical recommendations regarding the introduction of changes and additions to the current Criminal Procedure Code of Ukraine have been laid out;

– *the educational process* – during the teaching of the educational disciplines «Organization of the investigation of criminal offenses», «Criminal process», «Criminal science», «Operational investigative activity», as well as the preparation of textbooks, study guides and monographic studies (implementation acts of the National Academy of Internal Affairs from April 19, 2024);

– *scientific activity* – to improve the methodology of investigation of certain types of criminal offenses against property (implementation acts of the National Academy of Internal Affairs of May 27, 2024; of the Dnipro State University of Internal Affairs of May 30, 2024);

–*law enforcement activities* – to improve the methodology of investigation of certain types of criminal offenses against property (acts of implementation of the Department of Strategic Investigations in the Dnipropetrovsk region of the DSR of the National Police of Ukraine dated June 7, 2024, of the Main

Investigative Department of the National Police of Ukraine dated October 16, 2024).

Keywords: fraud, Internet banking, pre-trial investigation, banking operations, electronic transfer, cybercrimes, methodology, forensic characteristics, prevention, criminal offense, typical investigative situations, investigative (detective) actions, covert investigative (detective) actions.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані
основні наукові результати дисертації:

1. Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

2. Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

3. Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).

4. Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

5. Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

6. Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання

інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

Наукові праці, що засвідчують апробацію матеріалів дисертації:

7. Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

8. Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200.

9. Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової системи України* : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123.

10. Перхун С. О. До питання визначення обставин, які підлягають встановленню під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення* : матеріали Міжнар. наук.-практ. конф. (Київ, 13–14 берез. 2023 р.). Київ : Наук.-дослід. ін-т публіч. права, 2023. С. 131–133.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АТО	–	Антитерористична операція
ГУНП	–	Головне управління Національної поліції
ЕОМ	–	Електронно-обчислювальна машина
ЕОТ	–	Електронно-обчислювальна техніка
ЄРДР	–	Єдиний реєстр досудових розслідувань
ІТ	–	Інформаційні технології
КК	–	Кримінальний кодекс
КМЕ	–	Комп’ютерно-мережева експертиза
КПК	–	Кримінальний процесуальний кодекс
МВС	–	Міністерство внутрішніх справ
НПУ	–	Національна поліція України
НСРД	–	Негласна слідча (розшукова) дія
ОГ	–	Організовані групи
ООС	–	Операція об’єднаних сил
ОРЗ	–	Оперативно-розшукові заходи
ПКЕ	–	Програмно-комп’ютерна експертиза
ПК	–	Персональний комп’ютер
СКТЕ	–	Судова комп’ютерно-технічна експертиза
СОГ	–	Слідчо-оперативна група
СРД	–	Слідча (розшукова) дія
п.	–	Пункт
р.	–	Рік
с.	–	Сторінка (сторінки)
ст.	–	Стаття
ч.	–	Частина

ВСТУП

Обґрунтування вибору теми дослідження. В умовах воєнної агресії з боку росії триває втілення раніше започаткованих реформ щодо розбудови України як правової та незалежної держави з метою інтегрування до європейського співтовариства. Проте події останнього десятиліття засвідчують, що євроінтеграційні процеси відбуваються в досить складних умовах. Так, 12 квітня 2014 року Рада національної безпеки і оборони України ухвалила рішення про початок Антитерористичної операції, 2018 року на сході України було запроваджено операцію Об'єднаних сил. Крім того, стан нестабільності загострився 2020 року, коли на всій території країни було запроваджено карантинні заходи внаслідок поширення гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2. На початку 2022 року розпочалося повномасштабне вторгнення російської федерації на територію України. Попри складний період, інформаційні технології продовжували стрімко розвиватися в усьому світі, зокрема в Україні. Процеси діджиталізації позначилися майже на всіх сферах суспільного життя країни. В умовах виняткової політичної обстановки в державі злочинці суттєво вдосконалювали новітні способи та засоби вчинення протиправних діянь, спираючись на сучасні досягнення науки й техніки. Зважаючи на збільшення кількості внутрішньо переміщених осіб (біженців) унаслідок посилення «гарячої» фази бойових дій, спостерігається зростання кількості шахрайств у сфері використання інтернет-банкінгу. Шахраї використовують різноманітні схеми (фішинг, спамінг, кардинг) для заволодіння всіма грошовими коштами як громадян України, так й іноземців. За даними Офісу Генерального прокурора України, 2018 року до Єдиного реєстру досудових розслідувань було внесено 3366 фактів шахрайства за ч. 3 ст. 190 Кримінального кодексу України, з яких лише в 1120 випадках особам було вручено повідомлення про підозру; 2019 р. – 2467 фактів, повідомлення

про підозру – у 706 випадках; 2020 р. за ч. 2–4 ст. 190 КК України було внесено відомості в 14 744 випадках, з яких у 7734 випадках вручено повідомлення про підозру; 2021 р. – 9087 фактів, повідомлення про підозру – у 7634 випадках; 2022 р. – 19 430 фактів, повідомлення про підозру – у 6043 випадках; 2023 р. – 53 547 фактів, повідомлення про підозру – у 16 271 випадку; 2024 р. – 54 328 фактів, повідомлення про підозру – у 15 401 випадку; у І півріччі 2025 року було внесено 29 736 фактів, проте лише в 10 253 випадках особі було вручено повідомлення про підозру. Крім того, на сьогодні показники шахрайства у сфері використання е-банкінгу є досить високими, а кількість притягнутих до відповідальності дедалі зменшується.

Збільшення кількості шахрайств в умовах воєнного стану є особливо значущим, адже безліч шахрайських дій вчиняють стосовно військових, а також їхніх родичів, членів сім'ї та сумлінних громадян, які намагаються всіма доступними засобами наблизити перемогу. Крім того, своєчасне запобігання шахрайським виявам наразі є досить важливим для світового іміджу України. Таким чином, зазначене підтверджує потребу в розробленні сучасної методики розслідування шахрайства у сфері використання інтернет-банкінгу.

Наукову основу дисертаційного дослідження становлять ґрунтовні роботи дослідників з різних галузей юридичної науки, присвячені теоретичним засадам методики розслідування кримінальних правопорушень та її окремих структурних елементів, а саме: В. П. Бахіна, А. Ф. Волобуєва, В. Г. Дрозд, М. М. Єфімова, В. О. Коновалової, І. В. Пирога, О. В. Пчеліної, М. В. Салтевського, Р. Л. Степанюка, К. О. Чаплинського, Ю. М. Чорноус, В. Ю. Шепітька та ін.

Значний внесок у розроблення різних аспектів теоретико-прикладного забезпечення розслідування окремих видів шахрайства здійснили такі вчені, як: С. В. Головкін, А. Е. Жилін, В. Б. Коба, Т. В. Коршикова, О. В. Курман, Е. В. Малютін, В. Р. Мойсик, О. Л. Мусієнко, Т. В. Охрімчук, Н. В. Павлова, В. І. Пазиніч, Д. А. Птушкін, А. В. Рейнгольд, О. А. Самойленко,

С. В. Самойлов, В. В. Сисолятін, С. С. Чернявський, С. В. Чучко та ін.

Серед сучасних наукових розробок цієї проблематики можна виокремити дисертацію С. С. Кузьменка «Розслідування шахрайства, пов'язаного з інвестуванням коштів у будівництво об'єктів нерухомості» (м. Дніпро, 2019 р.), у якій автор визначив стан розроблення проблеми розслідування шахрайства; здійснив аналіз обстановки їх учинення; з'ясував криміналістично значущі ознаки особи шахрая та потерпілого (поведінкові детермінанти); схарактеризував форми взаємодії слідчого з оперативними підрозділами та сформував типові тактичні операції, спрямовані на виконання завдань розслідування шахрайства. У дисертації О. В. Доброової «Криміналістична характеристика та розслідування шахрайства з фінансовими ресурсами» (м. Київ, 2020 р.) здійснено аналіз шахрайства із фінансовими ресурсами як об'єкта криміналістичного дослідження; з'ясовано особливості виявлення злочинів і засади організації початкового етапу їх розслідування; окреслено типові слідчі ситуації, відповідні тактичні завдання та засоби їх вирішення. Своєю чергою Г. В. Захарова в дисертації «Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою» (м. Київ, 2021 р.) здійснила криміналістичний аналіз функціонування сфери туризму та визначила фактори, що зумовлюють шахрайські дії; запропонувала напрями забезпечення органами досудового розслідування заходів, спрямованих на відшкодування шкоди; з'ясувала особливості профілактичної діяльності уповноважених осіб у кримінальних провадженнях; сформувала типові тактичні операції, спрямовані на встановлення ознак організованості та викриття всіх співучасників шахрайства. Натомість І. О. Коваленко в дисертації «Розслідування шахрайства у сфері використання банківських електронних платежів» (м. Дніпро, 2022 р.) систематизував способи шахрайства; з'ясував зміст обстановки та слідової картини шахрайства; сформулював типові слідчі ситуації та відповідні їм комплекси слідчих (розшукових) дій (СРД) та негласних слідчих (розшукових) дій (НСРД).

Констатуючи наукову значущість наведених праць, варто наголосити, що дослідники опрацювали лише деякі проблемні аспекти зазначеної категорії кримінальних проваджень. Зокрема, невирішеними залишаються питання стосовно характеристики структури організованих груп та злочинних організацій, що вчиняють шахрайства; організації початкового й подальшого етапів розслідування; виокремлення особливостей використання спеціальних знань у кримінальному провадженні тощо. У сукупності окреслені фактори визначають актуальність вказаних питань, їх наукову та праксеологічну сутність, що зумовило вибір напряму дисертації.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до положень Стратегії національної безпеки України (Указ Президента України від 14 вересня 2020 р. № 392/2020), Стратегії кібербезпеки України (Указ Президента України від 14 травня 2021 р. № 447/2021), Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації (розпорядження Кабінету Міністрів України від 17 листопада 2021 р. № 1467-р), Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16 вересня 2020 р. № 1126-р), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 3 березня 2021 р. № 179), Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р), Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України (спільний наказ Офісу Генерального прокурора та МВС України від 22 листопада 2021 р. № 371/846), тематики наукових досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022–2026 роки (наказ МОН України від 3 лютого 2022 р. № 109), Основних напрямів наукових досліджень Науково-дослідного інституту публічного

права на 2020–2025 рр.

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає у вирішенні конкретного наукового завдання з розроблення теоретичних положень та криміналістичних рекомендацій щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу.

Комплексність мети, її багатоплановість обумовили необхідність вирішення окремих *завдань*:

– опрацювати ґенезу наукових поглядів щодо побудови методики розслідування шахрайства у сфері використання інтернет-банкінгу;

– з’ясувати концептуальні засади формування криміналістичної характеристики досліджуваного виду шахрайства;

– схарактеризувати основні елементи криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу;

– визначити особливості аналізу й оцінки первинної інформації, а також коло обставин, що підлягають встановленню в кримінальному провадженні;

– сформулювати типові слідчі ситуації, що виникають під час розслідування шахрайства у сфері використання інтернет-банкінгу, та надати алгоритми їх вирішення;

– конкретизувати особливості організації і тактики проведення процесуальних дій на початковому етапі розслідування шахрайства;

– розкрити організаційно-тактичне забезпечення проведення процесуальних дій на подальшому етапі розслідування шахрайства;

– визначити особливості використання спеціальних знань у кримінальному провадженні.

Об’єктом дослідження є кримінальні процесуальні відносини, що виникають у діяльності правоохоронних органів під час розслідування шахрайства у сфері використання інтернет-банкінгу.

Предмет дослідження – *теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-*

банкінгу.

Методи дослідження. Відповідно до поставленої мети, через призму об'єкта і предмета дослідження застосовано низку загальнонаукових і спеціальних методів наукового пізнання, основоположним серед яких є *діалектичний метод*. Так, *формально-логічні методи (аналіз, узагальнення, абстрагування, індукція тощо)* дозволили сформулювати фундаментальні визначення стосовно методики розслідування шахрайства у сфері використання інтернет-банкінгу (розділи 1, підрозділ 2.1), а також послідовно та ґрунтовно опрацювати інститут спеціальних знань, визначити його місце в криміналістичній категорії (підрозділи 3.3). *Системно-структурний метод* – для формулювання сутності та системи методики розслідування шахрайства, систематизації типових способів учинення та вузлових ділянок знаходження слідів, а також під час побудови типових слідчих ситуацій (розділ 1, підрозділ 2.1). *Порівняльно-правовий метод* – для аналізу кримінально-процесуальних і кримінальних норм, а також їх результатів для визначення способів учинення шахрайства (підрозділ 1.1). *Типологічний метод* – під час побудови «портрету» ймовірного шахрая, визначення структури організованої групи, яка вчиняє шахрайські дії у сфері використання інтернет-банкінгу, а також формулювання віктимогенних груп потерпілих (підрозділ 1.3). *Функціональний метод* – у межах встановлення алгоритмів проведення окремих СРД, НСРД та інших процесуальних дій для реалізації типових слідчих ситуацій розслідування шахрайства (підрозділи 2.2, 3.1, 3.2). *Догматичний* – під час тлумачення певних юридичних категорій, уточнення понятійного апарату (розділи 1–3). *Документальний, статистичний* та *соціологічний методи* – для узагальнення матеріалів судово-слідчої практики й аналізу опитування респондентів (підрозділи 1.2, 1.3, розділи 2 та 3), а також для виявлення тактичних помилок під час проведення СРД та НСРД на початковому й подальшому етапах розслідування шахрайства (підрозділи 3.1–3.2). Завдяки *синтезу* сформульовано загальні висновки (розділи 1–3).

Емпіричну основу дослідження становлять згруповані дані Єдиного звіту про вчинені кримінальні правопорушення Офісу Генерального прокурора України за 2018-й – І півріччя 2025 року та відомості аналізу судово-слідчої практики за цей період. Вивчено матеріали 236 кримінальних проваджень з проблематики дослідження (ч. 2–4 ст. 190 КК України) у таких областях, як Вінницька, Дніпропетровська, Закарпатська, Запорізька, Івано-Франківська, Київська, Кіровоградська, Львівська, Миколаївська, Одеська, Полтавська, Сумська, Тернопільська, Харківська, Хмельницька, Чернігівська та Черкаська, а також м. Київ. Крім того, проаналізовано результати опитування 227 працівників органів досудового розслідування, 142 працівників підрозділів дізнання, 224 співробітників оперативних підрозділів, 47 представників кіберполіції Національної поліції України, 88 працівників органів прокуратури та 71 працівника різних НДЕКЦ МВС України. Під час дослідження використано власний досвід роботи в правоохоронних органах України.

Наукова новизна одержаних результатів полягає в тому, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням теоретичних і практичних основ методики розслідування шахрайства у сфері використання інтернет-банкінгу, у якому сформульовано низку наукових положень, висновків 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:

вперше:

– запропоновано структуру злочинної організації, яка здійснює шахрайські дії у сфері використання інтернет-банкінгу, до якої входять такі групи осіб: 1) організатори; 2) адміністратори сайтів, де розміщують неправдиві відомості про товари або надання послуг; 3) продавці, які спілкуються з потенційними потерпілими (здебільшого через телефонні

розмови або sms-переписки); 4) спамери (особи, які здійснюють розсилку листів стосовно інтернет-магазинів з продажу товарів або надання різноманітних послуг); 5) фішери (особи, які розсилають листи для отримання особистої інформації потенційних потерпілих); 6) програмісти (особи, які створюють спам-боти для розсилки та віруси для потенційних атак); 7) хакери (особи, які здійснюють вірусні атаки на об'єкти, що зацікавили злочинну організацію); 8) охоронці; 9) корумповані представники органів державної влади й управління, працівники правоохоронних органів, які беруть участь у прикритті організованої злочинної діяльності;

– наведено низку тактичних завдань, які мають реалізувати уповноважені особи в досліджуваній категорії кримінальних проваджень, а також розроблено комплекси дій для їх вирішення в межах проведення початкового та подальшого етапів розслідування, зокрема: 1) тактичне завдання «Профілактика протиправних дій» – реалізація відповідних профілактичних заходів для усунення причин та умов учинення шахрайства у сфері використання інтернет-банкінгу; 2) тактичне завдання «Встановлення шахрая» – проведення низки процесуальних дій і заходів, спрямованих на виконання вказаного завдання; 3) тактичне завдання «Встановлення співучасників в організованій групі чи злочинній організації» – з'ясування ймовірної участі та ролі шахрая у відповідній структурі;

– надано пропозиції щодо внесення змін до ч. 1 ст. 71 КПК України та запропоновано викласти в такій редакції: «Спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками, що можуть бути застосовані під час досудового розслідування та судового розгляду шляхом надання довідок, пояснень, консультацій і висновків в усній чи письмовій формі для вирішення питань, що вимагають володіння відповідними спеціальними знаннями чи навичками»;

удосконалено:

– систему складових методики розслідування шахрайства у сфері використання інтернет-банкінгу, у якій виокремлено такі елементи:

криміналістична характеристика шахрайства; аналіз початкових відомостей та їхня оцінка; перелік обставин, що підлягають встановленню в кримінальному провадженні; типові слідчі ситуації, які формуються під час розслідування шахрайства, а також алгоритми їх реалізації; сукупність тактичних операцій для реалізації конкретних завдань розслідування; взаємодія уповноважених осіб з окремими підрозділами Національної поліції та іншими державними органами в кримінальному провадженні; профілактична діяльність уповноважених осіб у кримінальному провадженні; тактика проведення окремих СРД, НСРД та інших процесуальних дій на початковому етапі розслідування шахрайства у сфері використання інтернет-банкінгу; тактика проведення окремих СРД, НСРД та інших процесуальних дій на подальшому етапі розслідування; особливості використання спеціальних знань у кримінальному провадженні;

– сукупність інформаційних даних щодо обстановки вчинення шахрайства у сфері використання інтернет-банкінгу на основі опрацювання просторово-часових, економічних, психологічних і соціальних факторів;

– перелік потенційних місць учинення протиправних діянь: місця розташування електронно-обчислювальної техніки (ЕОТ), що були використані під час учинення кримінальних правопорушень (місце проживання підозрюваного, місця загального доступу); місця розміщення терміналів, банків, банкоматів та інших фінансових установ; місце перебування особи потерпілого, на яку були спрямовані шахрайські дії;

– сукупність даних стосовно матеріальних та особистісних слідів, а також виокремлення серед них особливої групи слідів, характерних для вчинення шахрайства у сфері використання інтернет-банкінгу – цифрових (електронних, віртуальних) слідів, які здебільшого виявляють у таких місцях: профілях соціальних мереж (Facebook, Instagram, Twiter), месенджерах (Telegram, Viber), застосунках для переписок криптовалютного спрямування (Binance), кеш-пам’яті онлайн магазинів, базах інтернет-провайдерів тощо;

– систему віктимогенних груп осіб, стосовно яких було вчинено

шахрайські дії, а саме: а) фізичні особи, які через шахрайські дії дозволили шахраям використовувати власні ЕОТ; б) родичі фізичних осіб, які через шахрайські дії надали дозвіл шахраям на використання власних ЕОТ; в) фізичні особи, які здійснювали торгівлю на онлайн платформах та інтернет-аукціонах з використанням інтернет-банкінгу;

– рекомендації стосовно аналізу початкової інформації для більш ефективної реалізації провадження завдяки правильній оцінці первинних даних та прийняття обґрунтованого рішення щодо початку досудового розслідування;

– систему типових слідчих ситуацій, що виникають під час розслідування шахрайства: вчинено шахрайські дії у сфері використання інтернет-банкінгу, є особистісна доказова база, шахрай відомий; вчинено шахрайські дії у сфері використання інтернет-банкінгу, є особистісна доказова база, шахрай невідомий; вчинено шахрайські дії у сфері використання інтернет-банкінгу, є особистісна та матеріальна доказова база, шахрай невідомий; вчинено шахрайські дії у сфері використання інтернет-банкінгу, повністю відсутня доказова база;

– перелік питань, які необхідно з’ясувати під час проведення допиту підозрюваного, а саме: які способи застосовувалися для входу в застосунок інтернет-банкінгу (використання спам-ботів; реквізитів картки, одержаної від конкретного потерпілого шляхом шахрайських дій; використання реквізитів картки, отриманої з web-сторінок підставних інтернет-магазинів); у який спосіб безпосередньо вчинено шахрайські дії (шляхом отримання доступу до ЕОТ з паролями, які встановив потерпілий; шляхом використання мережі Wi-Fi); чи вчинено шахрайські дії організованою групою або злочинною організацією; якщо так, то яка структура угруповання; який статус та обов’язки кожного з її учасників; яким чином розподілялися майно та грошові кошти між співучасниками; протягом якого проміжку часу було вчинено шахрайські дії; чи були скоєні супутні кримінальні правопорушення; які знаряддя й засоби використовувались під час учинення шахрайських дій

(комп'ютери, ноутбуки, смартфони, модеми, маршрутизатори, браузери, спам-боти); яка загальна сума грошових коштів була отримана шляхом реалізації шахрайських дій у сфері використання інтернет-банкінгу тощо;

дістали подальшого розвитку:

– теоретичні положення стосовно основних криміналістичних категорій (методика розслідування, криміналістична характеристика, обставини, які підлягають встановленню, типові слідчі ситуації, профілактична діяльність);

– структура криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу, у якій виокремлено такі елементи: спосіб підготовки, безпосереднього вчинення та приховування шахрайства; обстановка вчинення шахрайства у сфері використання інтернет-банкінгу; слідова картина протиправного діяння; особа шахрая; особа потерпілого;

– криміналістичне наповнення типових способів підготовки, безпосереднього вчинення та приховування шахрайства у сфері використання інтернет-банкінгу під час користування послугами в інтернет-магазинах, на різноманітних сайтах, зокрема фішинг, спамінг, кардінг;

– сукупність обставин, які необхідно встановлювати під час розслідування шахрайства у сфері використання інтернет-банкінгу, а саме: 1) обставини, що розкривають умови та способи вчинення шахрайства (інформація про час і місце його вчинення, відомості щодо способу підготовки, безпосереднього вчинення та приховування шахрайських дій, зокрема застосування спам-ботів, використання вірусних програм до ЕОТ потерпілих, використання різноманітних шахрайських схем), засоби, які використовували під час учинення шахрайських дій; 2) обставини, які характеризують особу злочинця або групу осіб (кількість шахраїв, розподіл серед них обов'язків, визначення їх ролі в організованій групі чи злочинній організації); 3) обставини, які характеризують особу потерпілого (віктимність її дій, базовий чи професійний користувач ЕОТ); 4) причиново-наслідкові зв'язки між діями шахраїв і результатами, які їх характеризують;

5) встановлення причин та умов, що сприяли вчиненню шахрайських дій; 6) обставини, які обтяжують або пом'якшують покарання; 7) вид і розмір шкоди, яка завдана шахрайськими діями; 8) обставини, які є приводом для звільнення шахрая від кримінальної відповідальності;

– перелік слідчих версій, які слід встановлювати під час розслідування, зокрема: 1) шахрайство у сфері використання інтернет-банкінгу вчинено з метою одержання матеріальної вигоди пересічним громадянином; 2) шахрайство вчинено з метою одержання матеріальної вигоди особою, яка володіє спеціальними знаннями у сфері інформаційних технологій («хакер», програміст, працівник ІТ-сфери); 3) шахрайство вчинено з метою одержання матеріальної вигоди особою (особами), що мали вільний доступ до ЕОТ; 4) шахрайство вчинено з метою одержання матеріальної вигоди групою осіб, яка займається шахрайськими схемами;

– формулювання типових слідчих ситуацій як системи відомостей про протиправну подію та обстановку її розслідування, що позначається на підборі та черговості проведення СРД, НСРД й інших процесуальних дій для найбільш ефективної реалізації конкретного етапу кримінального провадження;

– перелік місць, де доцільно проводити обшук, а саме: місця зберігання та обробки даних про використання інтернет-банкінгу (сервери відповідних банківських установ, ЕОТ шахраїв); місця знаходження ЕОТ, яку використовували для здійснення шахрайських дій; місця зберігання відомостей, отриманих злочинним шляхом.

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

– *законотворчій діяльності* – для вдосконалення законодавства у сфері використання банківських електронних платежів і запобігання кримінальним правопорушенням, пов'язаним із використанням інтернет-банкінгу, викладено низку практичних рекомендацій стосовно внесення змін і

доповнень до чинного Кримінального процесуального кодексу України;

– *освітньому процесі* – під час викладання навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Кримінальний процес», «Криміналістика», «Оперативно-розшукова діяльність», а також підготовки підручників, навчальних посібників і монографічних досліджень (акт впровадження Національної академії внутрішніх справ від 19 квітня 2024 р.);

– *науковій діяльності* – для вдосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Національної академії внутрішніх справ від 27 травня 2024 р., Дніпровського державного університету внутрішніх справ від 30 травня 2024 р.);

– *правозастосовній діяльності* – для вдосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Управління стратегічних розслідувань в Дніпропетровській області ДСР Національної поліції України від 07 червня 2024 р., Головного слідчого управління Національної поліції України від 16 жовтня 2024 р.).

Апробація результатів дисертації. Основні теоретичні положення й висновки дисертації оприлюднено на міжнародних науково-практичних конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 2020 р.), «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення » (м. Київ, 2021 р.), «Проблемні питання юридичної науки в контексті реформування правової системи України» (м. Київ, 2022 р.), «Пріоритетні напрями розвитку юридичної науки в умовах сьогодення» (м. Київ, 2023 р.).

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

доповідей, оприлюднених на міжнародних науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з основної частини (вступу, трьох розділів, що містять вісім підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 209 сторінок, з яких основного тексту – 141 сторінка. Список використаних джерел налічує 174 найменування – на 21 сторінці, 4 додатки – на 24-х сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ МЕТОДИКИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ ІНТЕРНЕТ-БАНКІНГУ

1.1. Ґенеза наукових поглядів щодо побудови методики розслідування шахрайства у сфері використання інтернет-банкінгу

Методика розслідування окремих видів кримінальних правопорушень як розділ криміналістики започаткувався на території України приблизно в середині ХХ-го сторіччя. На початку її розвитку створювалися методики по загальнокримінальним протиправним діянням: вбивствам, нанесенню тілесних ушкоджень, крадіжкам, грабежам, розбоям тощо. На межі ХХ-ХХІ століть розвиток інформаційних технологій та мережі Інтернет зумовив виникнення новітніх способів вчинення відомих кримінальних правопорушень (шахрайство, злочини у фінансовій сфері), а також появу нових складів протиправних діянь (наприклад, у сфері використання ЕОТ). З огляду на зазначене, виникла потреба побудови методики розслідування шахрайства у сфері використання інтернет-банкінгу як давнього складу кримінального правопорушення в поєднанні з новітніми способами його учинення [100, с. 164].

Для початку звернемося до позиції О. А. Антонюка, який акцентував увагу, що «…важливим є дослідження наукових розробок з приводу визначення особливостей регулювання кримінально-процесуальних відносин у сфері громадського порядку. Адже будь-яка структура повинна мати основу. На нашу думку, першочерговою основою методики розслідування кримінальних правопорушень є безпосередньо самі протиправні діяння, а також матеріали судово-слідчої практики щодо їх розслідування. Крім того,

важливе значення в даному теоретичному аспекті криміналістики займають різноманітні праці науковців з приводу зазначеної проблематики. Тому їх дослідження, а також вивчення кримінальних справ й проваджень, надало змогу з'ясувати сутність й структуру досліджуваної методики розслідування» [4, с. 249].

В розрізі визначеної проблематики, вважаємо доречною тезу І. О. Коваленка, який зауважував, що «…досить велика кількість протиправних діянь якраз вчинюється у сфері власності (крадіжки, грабежі, розбої, шахрайства). Слід наголосити, що протягом останнього десятиріччя в Україні та в усьому світі інформаційні технології зробили великий крок вперед, що стало одним з вагомих чинників загострення криміногенної ситуації у сфері банківської діяльності. Адже з масовою комп'ютеризацією та використанням всесвітньої мережі Інтернет діяльність злочинного середовища набула відповідні зміни як серед новітніх способів учинення протиправних діянь, так і серед засобів їх учинення. Крім того, у зв'язку з розвитком банківської системи України, використанням в банківській діяльності таких продуктів як Internet Banking, Клієнт-Банк та інші збільшилася кількість кримінальних правопорушень в сфері банківських електронних платежів. З огляду на складність кримінальних проваджень досліджуваної категорії, як у всьому світі, так і в Україні, виникає необхідність у створенні сучасної методики розслідування вказаних протиправних діянь» [35, с. 84]. Ми підтримуємо вищенаведені позиції, та вважаємо актуальним розробку дієвої методики розслідування шахрайства у сфері використання інтернет-банкінгу.

Загалом стосовно методики розслідування кримінальних правопорушень, то, для прикладу, А. П. Шеремет, відмічав наступне: «…методика розслідування злочинів – це самостійний розділ науки криміналістики. Його складають основані на вимогах кримінального і кримінально-процесуального законодавства наукові положення, рекомендації і методи розслідування окремих видів злочинів. Вчені криміналісти методику

розслідування злочинів розглядають у двох аспектах: 1) це сам процес розслідування злочинів, що здійснюється на підставі застосування засобів криміналістичної техніки, прийомів слідчої тактики, методів розслідування певних видів злочинів; 2) це розділ науки криміналістики, який містить систему комплексних криміналістичних рекомендацій щодо виявлення, розслідування та профілактики окремих видів злочинів. Саме у взаємозв'язку цих двох напрямів (практичного і теоретичного) методика розслідування злочинів виявляє своє призначення, сприяючи розробленню наукових рекомендацій і запровадженню їх у практику розслідування злочинів» [169, с. 330]. Поділяючи наведену думку, звернемося до робіт представників різних шкіл вітчизняних учених-криміналістів.

Зокрема, вважаємо доречним твердження Ю. М. Чорноус, яка вказала, що «…криміналістичне забезпечення розслідування кримінальних правопорушень завжди було і є одним із пріоритетних напрямів розвитку науки криміналістики. Важливо, що саме за змістом криміналістичної методики, як особливого розділу науки криміналістики, аналізується накопичений досвід слідчої, експертної, судової практики, відшукуються найефективніші прийоми, методи та засоби розслідування та попередження різних категорій кримінальних правопорушень. Розроблені наукою криміналістичні рекомендації є важливим інструментарієм слідчого, інших компетентних суб'єктів, що залученні до кримінального провадження – своєрідним алгоритмом дій у типових слідчих ситуаціях. Подія кримінального правопорушення, як і будь-яке явище об'єктивної дійсності, є індивідуальною та неповторною. Тому її пізнання також відрізняється специфічними індивідуальними рисами. Разом з тим, кожне кримінальне правопорушення та особливості проведення досудового розслідування мають повторювані ознаки, що в свою чергу служать основою формування та розробки типових прийомів розслідування як в цілому, так і щодо однорідних за криміналістичною характеристикою кримінальних правопорушень» [59, с. 567].

Зі свого боку, В. Ю. Шепітько вдало наголошував на тому, що «…методика розслідування окремих видів злочинів (або криміналістична методика) є важливим розділом науки криміналістики. Криміналістична методика – це система наукових положень і розроблюваних на їх основі рекомендацій щодо організації і здійснення розслідування та запобігання окремих видів злочинів. У системі криміналістичних знань вона являє собою синтезуючий рівень, який об'єднує положення криміналістичної техніки і криміналістичної тактики в їх переломленні до умов розслідування певного виду злочину. У теорії криміналістики слід розрізняти поняття методу і методики. Під методами маються на увазі способи практичного здійснення чого-небудь, досягнення певних результатів (їх комплекси), спрямовані на збирання, дослідження та оцінку доказів з метою встановлення істини по кримінальній справі. Методика – це сукупність методів (їх система), в якій вони пов'язані між собою і підпорядковані певній меті розслідування злочинів» [61, с. 269]. Тобто автор вказував на можливість сприйняття методики в двох іпостасях: як системи методів та як системи рекомендацій на основі наукових положень для розслідування протиправних діянь.

В свою чергу, колектив львівських учених-криміналістів зауважував, що «…у криміналістичній науці не має єдиного визначення криміналістичної методики. Водночас ідеться не стільки про існування принципово відмінних понять, скільки про своєрідне авторське трактування одного й того ж об'єкта пізнання засобами спеціальної юридичної лексики у цій сфері. Загалом більшість сучасних учених-криміналістів розглядають криміналістичну методику в двох аспектах – теорії та практики. Відповідно до цього поділу йдеться про два основні підходи до розуміння сутності криміналістичної методики: а) криміналістична методика – розділ криміналістики, предметом якого є вивчення теоретичних положень і практичних рекомендацій щодо організації, керівництва, планування і провадження виявлення та розслідування окремих видів злочинів (кримінальних правопорушень); б) криміналістична методика – науково обґрунтований процес застосування у

практичній діяльності органів досудового слідства криміналістичних методів і засобів розслідування певних видів злочинів (кримінальних правопорушень)» [60, с. 499-500]. Як бачимо, думки двох груп дослідників з різних наукових шкіл (львівської та харківської) майже ідентичні.

Також приведемо твердження київської школи криміналістів, які вказали, що «…назва завершального розділу криміналістики «криміналістична методика» лише умовно передає сутність змістовного навантаження, що охоплює поняття «методика». В криміналістичній методиці розроблюються та рекомендуються до застосування під час розслідування не тільки певні методи, засоби і прийоми діяльності, але й положення, які стосуються: криміналістичної характеристики відповідного виду кримінальних правопорушень; типових слідчих ситуацій; типових переліків обставин, що потребують встановлення; напрямів взаємодії слідчого з іншими учасниками розслідування, правоохоронними та державними органами тощо. Такі рекомендації являють собою програми розслідування за похідною типовою слідчою ситуацією і визначають коло завдань, що вирішуються за допомогою відповідних алгоритмів дій слідчого, тим самим набуваючи технологічного характеру. Криміналістична методика – це завершальний розділ науки криміналістики, що представляє собою систему наукових положень і сформованих на їх основі практичних рекомендацій, що забезпечують ефективність діяльності слідчого та інших компетентних суб'єктів з розслідування та попередження окремих видів кримінальних правопорушень» [59, с. 569].

А представники дніпровської школи криміналістики вказували наступне: «Криміналістична методика» – назва заключного розділу науки «криміналістика», що разом з іншими її частинами утворює єдину систему знань. Порівняно з іншими, зокрема, криміналістичними технікою та тактикою, розділ було виділено пізніше. .... Криміналістична методика, будучи заключним розділом криміналістики, поєднує теоретичні положення і практичні рекомендації, викладені в попередніх розділах науки, пропонує, як

використовувати досягнення криміналістичної техніки і тактики при розслідуванні злочинів залежно від їх видової чи групової належності. Таким чином, можна сказати, що криміналістичні техніка і тактика співвідносяться з криміналістичною методикою як загальна й особлива частини науки. Щоб успішно вирішувати завдання розслідування конкретного посягання, необхідно опановувати слідчу практику, мати в своєму розпорядженні дані щодо досвіду розкриття подібних діянь. Будь-який злочин індивідуальний і неповторний, однак у кожному зустрічаються схожі ознаки, що служать основою для визначення і розробки типових прийомів розслідування. Тож, в межах криміналістичної методики досліджується слідча практика по різних видах злочинів, досвід ефективного використання тактичних прийомів, науково-технічних засобів, що дозволяє розробляти систему рекомендацій з проведення розслідування, враховуючи особливості злочинів окремих видів чи груп» [58, с. 340]. Тобто всі наведені представники різних шкіл криміналістів незалежної України визначають криміналістичну методику в двох формах: як заключний розділ криміналістики та як систему науково-обґрунтованих рекомендацій по розслідуванню окремих видів кримінальних правопорушень.

А вже А. П. Шеремет зазначав, що «…методика розслідування окремого виду злочину або окрема методика становить систему положень та наукових рекомендацій, які визначають порядок діяльності слідчого під час розслідування окремого виду злочину. Для кожного виду злочину існують структурні схеми, алгоритми діяльності, які придатні для розслідування будь-якого виду злочинів. Такі алгоритми діяльності називають структурою окремої методики. Вона включає такі елементи: криміналістичну характеристику даного виду злочинів; обставини, які необхідно встановити; особливості порушення кримінальної справи; першочергові слідчі дії та оперативно-розшукові заходи; типові слідчі ситуації, типові версії та планування; тактику провадження окремих слідчих дій; профілактичні слідчі дії. Врахування перелічених елементів під час розслідування злочинів

дозволяє визначати напрями розслідування та оптимізувати діяльність слідчого» [169, с. 335].

В свою чергу, Ю. М. Чорноус зауважила, що при всьому різноманітті окремих методик вони мають певні типові елементи. Авторка вказала, що «…типова структура окремої криміналістичної методики, як правило, складається з наступних взаємопов'язаних частин: криміналістична характеристика даного виду кримінальних правопорушень; типовий перелік обставин, що підлягає встановленню під час розслідування кримінальних правопорушень даного виду (групи); типовий алгоритм (план) слідчих і негласних слідчих (розшукових), інших процесуальних дій та інших заходів на кожному етапі розслідування з урахуванням типових слідчих ситуацій; особливості тактики проведення окремих слідчих (розшукових), інших процесуальних дій, тактичних операцій (комбінацій); особливості використання спеціальних знань у кримінальних провадженнях даної категорії; особливості взаємодії слідчого з оперативними підрозділами Національної поліції, інших правоохоронними органами, державними органами, установами та організаціями у кримінальних провадженнях даної категорії; особливості залучення допомоги населення та використання можливостей засобів масової інформації під час розслідування кримінальних правопорушень даного виду (групи); особливості профілактичної діяльності слідчого, інших компетентних суб'єктів у кримінальних провадженнях даної категорії» [59, с. 576].

Зі свого боку, О. В. Лускатов виділив наступні складові в структурі окремої криміналістичної методики, зокрема: «…1) криміналістична характеристика злочину окремого виду (групи); 2) організація та планування розслідування на початковому етапі стосовно до існуючих типових слідчих ситуацій; 3) слідчі (розшукові) й інші дії та заходи відповідно до типових слідчих ситуацій на подальшому етапі розслідування; 4) профілактична діяльність слідчого» [58, с. 346].

З огляду на зміни законодавства та загалом реформування

правоохоронної системи України М. М. Єфімов сформував таку структуру досліджуваної наукової категорії, як-от: «…криміналістична характеристика злочинів; аналіз первинної інформації та початок кримінального провадження; обставини, що підлягають доведенню по кримінальному провадженню; типові слідчі ситуації розслідування; особливості проведення початкових слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів; особливості проведення подальших слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів; особливості використання спеціальних знань під час розслідування кримінального правопорушення; профілактична діяльність слідчого стосовно причин та умов, що сприяли вчиненню кримінального правопорушення; особливості діяльності слідчого на завершальному етапі розслідування» [19, с. 13-14].

Якщо ж говорити про розслідування кримінальних правопорушень визначеної категорії, то, для прикладу, І. О. Коваленко в методиці розслідування шахрайства у сфері використання банківських електронних платежів виділив такі складові: криміналістична характеристика; аналіз та оцінка початкової інформації, а також коло обставин, котрі підлягають встановленню; типові слідчі ситуації та відповідні їм алгоритми дій працівників правоохоронних органів під час розслідування досліджуваної категорії кримінальних правопорушень; організація і тактика проведення окремих слідчих (розшукових) дій; організаційно-тактичні аспекти проведення негласних слідчих (розшукових) дій; особливості призначення експертиз в кримінальних провадженнях досліджуваної категорії [44]. А вже С. В. Чучко визначив у методиці розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет такі елементи як: правове регулювання правовідносин у віртуальному просторі та криміналістичний аналіз шахрайства у мережі Інтернет; криміналістичну характеристику; оцінка первісної інформації та коло обставин, що підлягають встановленню; типові слідчі ситуації; взаємодія слідчих та оперативних підрозділів Національної поліції при розслідуванні шахрайства при купівлі-продажу

товарів через мережу Інтернет; проведення слідчих (розшукових) дій, спрямованих на вилучення інформації з матеріальних джерел; проведення слідчих (розшукових) дій, спрямованих на вилучення інформації з особистісних джерел; особливості використання спеціальних знань при розслідуванні шахрайств при купівлі-продажу товарів через мережу Інтернет» [172, с. 235].

Досить цікавою є побудова методики розслідування шахрайства у сфері використання банківських електронних платежів, надана А. Е. Жиліним, який виокремив в ній наступні складові: стан наукових досліджень питань протидії шахрайствам у сфері використання банківських електронних платежів; криміналістична характеристика; криміналістичний аналіз первісної інформації та визначення основних напрямів розслідування; взаємодія слідчих та працівників оперативних підрозділів Національної поліції у кримінальному провадженні; профілактична діяльність працівників правоохоронних органів щодо виявлення й усунення причин та умов учинення шахрайства у сфері використання банківських електронних платежів; тактичні операції [24].

Наостанок приведемо сформовану А. В. Рейнгольдом структуру методики розслідування шахрайства в інтернет-комерції, а саме: стан наукових досліджень проблем боротьби із кібер-шахрайством та правові передумови виникнення інтернет-комерції; криміналістична характеристика шахрайства в інтернет-комерції; оцінка первинної інформації на початку кримінального провадження; організація та планування розслідування шахрайства в інтернет-комерції, та коло обставин, що підлягають встановленню; типові слідчі ситуації, що виникають під час досудового розслідування шахрайства в інтернет-комерції; проведення окремих слідчих (розшукових) та процесуальних дій; криміналістична профілактика у кримінальних провадженнях за фактами вчинення шахрайства в інтернет-комерції; застосування тактичних операцій під час розслідування шахрайства в інтернет-комерції [116, с. 381]. Як бачимо, всі наведені структури мають як

набір загальноприйнятих елементів (криміналістична характеристика, типові слідчі ситуації), так і специфічні (стан наукових досліджень питань протидії шахрайствам у сфері використання банківських електронних платежів, правове регулювання правовідносин у віртуальному просторі та криміналістичний аналіз шахрайства у мережі Інтернет).

Опрацювання вищенаведених досліджень науковців, а також аналіз матеріалів кримінальних проваджень дозволило нам побудувати методику розслідування шахрайства у сфері використання інтернет-банкінгу, в якій було вирізнено такі складові, як-от:

– криміналістична характеристика шахрайства у сфері використання інтернет-банкінгу;

– аналіз початкових відомостей та їх оцінка;

– перелік обставин, що необхідно встановлювати в кримінальних провадженнях досліджуваної категорії;

– типові слідчі ситуації, які формуються під час розслідування досліджуваного протиправного діяння, а також алгоритми їх реалізації;

– сукупність тактичних операцій для реалізації конкретних завдань розслідування;

– взаємодія уповноважених осіб з окремими підрозділами Національної поліції та інших держаних органів у кримінальному провадженні досліджуваної категорії;

– профілактична діяльність уповноважених осіб у кримінальних провадженнях досліджуваної категорії;

– тактика проведення окремих СРД, НСРД та інших процесуальних дій на початковому етапі розслідування шахрайства у сфері використання інтернет-банкінгу;

– тактика проведення окремих СРД, НСРД та інших процесуальних дій на подальшому етапі під час розслідування протиправних діянь;

– особливості використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу.

Констатуючи вищенаведене, зазначимо, що на разі існує потреба побудови методики розслідування шахрайства у сфері використання інтернет-банкінгу як давнього складу кримінального правопорушення в поєднанні з новітніми способами його учинення. Опрацювання вищенаведених досліджень науковців, а також аналіз матеріалів кримінальних проваджень дозволило нам побудувати методику розслідування шахрайства у сфері використання інтернет-банкінгу, в якій було вирізнено певні складові.

1.2. Концептуальні засади формування криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу

Криміналістична характеристика є відносно новою науковою категорією. Перші згадки про неї почалися в 60-70-их роках минулого сторіччя. З того ж часу постійно відбуваються наукові дискусії між різними науковцями з приводу як сутності та структури, так і загалом стосовно доцільності її входження в методику розслідування. Ми підтримуємо позицію групи вчених-криміналістів, які вказують на беззаперечну обов’язковість дослідження криміналістичної характеристики. Тому в нашій роботі буде опрацьовано визначену наукову категорію як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу [99, с. 805].

Для початку приведемо позицію С. В. Чучка, який зауважив, що «…еволюційні зміни внаслідок розвитку інноваційних технологій та впровадження їх у всі сфери життєдіяльності, торкнулися й глобальної мережі Інтернет, без якої її користувачі не уявляють існування. Останні десятиріччя відбувається стрімкий зріст правочинів через мережу Інтернет, за допомогою якого можна здійснити операції побутового та комерційного призначення та придбати товар, не залишаючи місця проживання. Для

більшості населення така форма «віртуальної» торгівлі стала зручною та істотно зекономила час, особливо у період пандемії, коли ряд торгівельних мереж змушені були переходити на дистанційний формат здійснення угод купівлі-продажу товарів та послуг. Проте, форми цивільних правовідносин в Інтернеті наразі є не досить врегульованими, що тягне за собою значну кількість порушень, зокрема й у сфері торгівлі товарами і послугами. Чимало цивільно-правових угод укладається через обман та зловживання довірою, що не лише порушує встановлений порядок їх здійснення, а і завдає шкоди майновим інтересам громадян» [167, с. 79].

Цікавою є думка О. І Миргородського стосовно того, що «…дані злочини, по-перше, все ж таки продовжували фіксуватись на території України, а, по-друге, відповідні діяння давно стали глобальною (міжнародною) проблемою, адже популярність комп'ютерних шахрайств невпинно зростає у всьому світі. Тому навіть у випадках позитивної динаміки поширення цих кримінальних правопорушень важливо, щоб суб'єкти запобігання злочинності (як загальні, так і спеціальні), продовжували вживати комплекс ефективних заходів запобігання названим суспільно небезпечним діянням (втрата пильності може призвести до неконтрольованих процесів у цьому напрямі)» [81, с. 453].

Як вірно відмічає М. М. Єфімов, «…будь-яка методика розслідування окремих видів кримінальних правопорушень має певну структуру, важливим елементом якої є криміналістична характеристика. Поняття криміналістичної характеристики як елемента методики, кількість, зміст і значення структурних елементів цієї наукової категорії залишаються невизначеними та суперечливими. Більше того, на рубежі тисячоліть гостро постало питання щодо доцільності існування криміналістичної характеристики як наукової категорії загалом. Також маємо зазначити, що значення криміналістичної характеристики можна розділити на практичне та теоретичне. Для працівників поліції, які безпосередньо займаються розслідуванням, найбільш важливим є практичне застосування того чи іншого засобу, що допоможе у

процесі розслідування. Тобто дійсна цінність криміналістичної характеристики того чи іншого виду кримінального правопорушення – це можливість її практичного застосування, можливість вирішити певні питання з огляду на неї та, звичайно, можливість, спираючись на неї, спростити розслідування певної категорії протиправних діянь» [17, с. 161]. І дійсно, ми також поділяємо думку, що реальне значення досліджуваної наукової категорії в можливості її практичного використання, тим більше під час розслідування шахрайства у сфері використання інтернет-банкінгу.

А вже Т. В. Вискарка зазначає, що «…криміналістична характеристика є відносно новою категорією в сучасній криміналістиці, оскільки перші згадки про неї почалися лише в сімдесятих роках минулого сторіччя. Найбільшого розквіту її дослідження на теренах української науки почалося приблизно з 2010 року. Саме тоді переважна кількість науковців-криміналісти під час висвітлення питань окремих методик розслідування кримінальних правопорушень вважали за необхідне розглянути і вказану складову. Як наслідок, зазначена категорія стала невід'ємною частиною будь-якої окремої методики. Тому вважаємо за потребу дослідити криміналістичну характеристику як елемент методики розслідування шахрайства у сфері використання банківських електронних платежів» [10, с. 106].

Наразі Ю. М. Чорноус акцентує увагу на тому, що «…розрізняють наступні характеристики кримінального правопорушення: кримінально-правову, криміналістичну, кримінологічну тощо. Кримінально-правова характеристика – це опис ознак, які надають уявлення щодо поняття кримінального правопорушення, а саме злочину та проступку, визначають їх спільні та відмінні ознаки. Важливою є класифікація кримінальних правопорушень за видами, ступенем небезпеки тощо. Кримінологічна характеристика – опис генезису кримінального правопорушення, його причин, умов вчинення, частоти повторюваності, розподілення кримінального правопорушення за іншими ознаками, наприклад, віком,

часом, територією тощо. Криміналістична характеристика взаємопов'язана з елементами інших характеристик та використовує їх відомості. Зокрема, предмет безпосереднього посягання включає кримінально-правову характеристику предмета, а опис особи злочинця у більшості методик межує з кримінологічною характеристикою. Криміналістична характеристика складає опис властивостей та ознак, які мають значення для розкриття механізму кримінального правопорушення, характеру слідів, що залишились, умов вчинення кримінального правопорушення та характеристики особи підозрюваного у його вчиненні» [59, с. 577-578]. Як бачимо, дослідниця вказує на обов'язковість опрацювання криміналістичної характеристики з огляду на її практичну значимість.

Досить вдало А. П. Шеремет підкресли, що «…значення криміналістичної характеристики полягає в тому, що вона дозволяє: визначити напрями розслідування; цілеспрямовано збирати доказову інформацію та її джерела; будувати найбільш вірогідні версії стосовно обставин, які необхідно встановлювати. Під час побудови методики криміналістичну характеристику використовують в кількісній залежності між такими елементами: «предмет – особа», «спосіб – особа», «предмет –спосіб», «слідова картина – особа злочинця», «предмет – сліди» тощо. Видова кількісна залежність між цими парами елементів під час планування та висунення версій переноситься на аналогічні пари елементів конкретного злочину. Таким чином, версії будуть найбільш вірогідними, а плани розслідування – більш оптимальними» [169, с. 342]. Тобто вчений-криміналіст більш розширив вказане попередньою дослідницею практичне значення визначеної наукової категорії, що, звичайно, корелюється і з розслідуванням шахрайства у сфері використання інтернет-банкінгу. Ми вважаємо, що криміналістичну характеристику в кримінальних провадженнях досліджуваної категорії можна застосовувати для висунення відповідних версій та під час проведення окремих СРД на будь-якому етапі розслідування.

А вже О. І Миргородський вказує на те, що «…відповідна диспропорція, через яку кількість зареєстрованих актів шахрайств (у тому числі вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки) суттєво зросла, а кількість злочинів та кримінальних правопорушень, в яких особам вручено повідомлення про підозру, навпаки, зменшилась, знову ж таки пояснюється впливом широкомасштабної війни, яку розгорнула держава-варвар проти України. Отже, війна негативним чином впливає на динаміку названого злочину, проте враховуючи той факт, що у багатьох випадках вчинення шахрайств шляхом незаконних операцій з використанням електронно-обчислювальної техніки суб'єкт кримінального правопорушення перебуває на тимчасово окупованих територіях або на території російської федерації, встановити особу винного та притягнути його до відповідальності надзвичайно складно» [83, с. 172].

Г. М. Яровенко та М. М. Бояджян досить правильно зазначили, що «…здійснення кібершахрайських операцій з банківськими картками та різними платіжними операціями має негативні наслідки для стабільності фінансової системи держави. Це проявляється у гальмуванні поширення безготівкової форми оплати, зниженні довіри населення до банків у частині зберігання коштів та кредитування. Недостатні знання про механізми кіберзлочинів ускладнюють процес визначення шахрайства. Вивчення ознак шахрайства, в першу чергу, необхідно для розробки більш дієвих засобів і методів захисту від даного виду злочину. Аналіз наслідків кібершахрайств дозволяє виявити слабкі місця в банківській системі та сприяє накопиченню інформації щодо способів, методів шахрайства, портретів шахраїв та їх жертв, формування ознак шахрайства. У результаті проведеного в статті аналізу виявлено, що збитки банків У результаті кібершахрайств зростають, не дивлячись на заходи служб безпеки. Клієнти та банки втрачають кошти завдяки різним шахрайським способам, серед яких найбільшої шкоди завдають методи соціальної інженерії. Для боротьби з такого роду шахрайствами запропоновано ряд заходів, реалізація яких потребує

застосування методів Data Mining та розвинутих інформаційних технологій» [171, с. 841].

Досить доречною вважаємо думку О. В. Пчеліної, яка відмітила, що «…ефективність і оптимізація розслідування як пізнавальної діяльності та методу боротьби зі злочинністю напряму залежать від наявності та стану розробленості відповідних криміналістичних рекомендацій. Останні знаходять свій вираз безпосередньо в криміналістичних методиках розслідування злочинів. Відповідні методики повинні бути дієвими, тобто виконувати своє функціональне призначення по відношенню до провадження досудового розслідування. А це неможливо без з'ясування сутності та вимог до її структурних елементів. Серед таких елементів слід виділити криміналістичну характеристику злочинів. Ця категорія є вкрай спірною та неоднозначною в криміналістичній науці, що, звичайно, не може не позначитися на якості криміналістичних методик, а значить і на якості розслідування злочинів. У зв'язку з цим вважаємо актуальним питанням щодо з'ясування сутності, змісту, значення та місця криміналістичної характеристики злочинів у криміналістиці в цілому та криміналістичній методиці зокрема» [113, с. 90].

Наразі М. М. Єфімов надав наступне формулювання криміналістичної характеристики «…як системи відомостей про криміналістично значущі ознаки протиправного діяння, яка відображає закономірні зв'язки між ними, слугує побудові та перевірці слідчих версій для вирішення основних завдань розслідування». Крім того, науковець наголосив, що «…визначена наукова категорія є динамічною. Іншими словами, вона може змінюватись залежно від конкретних умов дійсності, проте її використання може мати різні напрямки у діяльності працівників правоохоронних органів. Наприклад, за ознаками способу, місця та часу його вчинення може бути висунута версія щодо особи злочинця, і навпаки, при затриманні правопорушника та в разі наявності даних про обставини правопорушення може бути побудована версія про вчинення цією особою інших, ще не розкритих діянь» [18, с. 52-

53].

Також дещо своєрідною є позиція О. В. Одерія, який вказав, що «…криміналістичну характеристику, яка увійшла в науковий апарат криміналістики у 60-роках XX ст., на сьогодні розглядають у двох значеннях: як теоретичну основу формування окремих методик розслідування окремих видів (груп) злочинів і як робочий інструментарій слідчого, який він використовує під час розслідування конкретного злочинного вияву. У зв'язку з цим криміналістична характеристика стала невід'ємним і традиційно початковим елементом у структурі криміналістичних методик розслідування злочинів» [91, с. 93]. Ми повністю поділяємо вказану позицію, оскільки вважаємо, що дійсно криміналістична характеристика є першою складовою в методикам розслідувань окремих видів протиправних діянь.

А вже В. В. Тіщенко вказував, що «…для визначення кола елементів криміналістичної характеристики злочинів необхідно дотримуватися, принаймні, двох умов. Перша: набір її елементів повинен бути системним, що забезпечує повноцінне функціонування розглянутого поняття й відбиває основні закономірності у механізмі такого функціонування. Друга: виділені елементи повинні мати здатність нести інформацію про зміст і значення слідів-відображень і механізм їхнього утворення, відбивати можливості побудови моделі події в цілому чи окремих елементів при дефіциті інформації, щодо окремих обставин, особливостей взаємозв'язку і відносин між ними, показувати таким чином шляхи та засоби пізнання розслідуваної події» [151, с. 274].

Доволі доречною в розрізі наведеного вважаємо думку О. В. Лускатова, який відзначив, що «…криміналістична характеристика злочину являє собою інформаційну модель, узагальнене поняття, що містить ознаки, властиві одному виду (або групі схожих) злочинів. Вона є результатом дослідження та узагальнення матеріалів кримінальних проваджень з розслідування злочинів окремого виду. Практичне значення даної категорії в тім, що слідчий може використовувати її як модель (матрицю), шляхом перенесення даних, які її

складають, на конкретну подію, що дозволяє прогнозувати зміст окремих, ще не встановлених складових механізму вчинення цього злочину, а в підсумку дозволяє визначити методи, прийоми і засоби досягнення мети розслідування. Криміналістична характеристика також служить теоретичною базою для побудови методики розслідування» [58, с. 346].

Зокрема, М. М. Єфімов зауважив, що «…криміналістична характеристика злочинів є категорією динамічною. Іншими словами, вона може змінюватись залежно від конкретних умов дійсності. Проте її використання може мати різні напрямки у діяльності працівників правоохоронних органів. Наприклад, за ознаками способу, місця та часу його вчинення може бути висунута версія щодо особи злочинця і, навпаки, при затриманні правопорушника та наявності даних про обставини злочину може бути побудована версія про вчинення цією особою інших, ще нерозкритих злочинів. Отже, криміналістична характеристика злочинів – це система відомостей про криміналістично значущі ознаки кримінально караного діяння, яка відображає закономірні зв’язки між ними і слугує побудові та перевірці слідчих версій для вирішення основних завдань розслідування» [19, с. 14-15]. Також вважаємо відносно вірним визначення І. О. Коваленка, який підсумовуючи результати власного дослідження надав власне «…поняття криміналістичної характеристики як інформаційної моделі групи протиправних діянь певної категорії, яка має виражені складові зі сталими кореляційними зв’язками, що можуть використовуватись на будь-якому етапі розслідування» [37, с. 79]. Відтак, більш вдалим вбачаємо формулювання, надане окремою групою дослідників під керівництвом Є. В. Пряхіна: «…Криміналістична характеристика злочинів – заснована на практиці правоохоронних органів і криміналістичних досліджень модель системи зведених відомостей про криміналістично значущі ознаки виду, групи або конкретного кримінального правопорушення, яка має на меті оптимізувати процес його розслідування» [60, с. 507].

Отже, надамо власне авторське визначення криміналістичної

характеристики як сформованої ґрунтуючись на судово-слідчій практиці і дослідженнях науковців із різних юридичних галузей сукупності інформаційних даних про криміналістично значимі властивості та ознаки конкретного кримінального правопорушення (виду, групи), що мають сталі кореляційні зв'язки, а також що має на меті допомогу в попередженні й розслідуванні окремих категорій протиправних діянь.

Опрацьовуючи питання наповнення елементами криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу слід наголосити, що різні дослідники досить різнопланово підходили до вказаної проблематики. Зокрема, кількість складових визначеної наукової категорії варіювалась від чотирьох до більше ніж двадцяти. В той же час, ми вважаємо доцільним вводити в криміналістичну характеристику лише ті елементи, які мають між собою сталі кореляційні зв'язки та реальне розшукове значення.

Для початку приведемо твердження окремої групи науковців (В. С. Кузьмічова, Г. І. Прокопенка), які визначили серед її складових такі, як-от: «…предмет безпосереднього злочинного посягання (найрізноманітніші об'єкти органічного та неорганічного походження); спосіб вчинення злочинів в його широкому розумінні (обставини приготування, вчинення і приховування злочину, образ дії суб'єкта, що використовується для досягнення поставленої мети); типову «слідову картину» злочину в її широкій інтерпретації (сукупність джерел матеріальних та ідеальних відображень у навколишній матеріальній обстановці вчиненого злочину); особу злочинця (опис людини як соціально-біологічної системи, властивості та ознаки якої відображуються у матеріальному середовищі); особу потерпілого (для окремих видів чи груп злочинів: демографічні дані, відомості про спосіб життя, риси характеру, звички, зв'язки і стосунки, ознаки віктимності тощо)» [67, с. 253].

Наразі А. Ф. Волобуєв, О. В. Одерій та Р. Л. Степанюк вказали на те, що досліджувана наукова категорія повинна нараховувати такі складові: «…предмет злочину (гроші, матеріальні цінності, наркотичні речовини

тощо); місце, час та обстановка, характерні для вчинення злочинів окремих видів; способи підготовки, вчинення та приховування злочинів – певна система дій, прийомів та окремих операцій злочинців, у т.ч. використання знаряддя злочину (автотранспорту, вогнепальної й холодної зброї, знарядь зламу, обладнання для виготовлення фальшивих документів тощо); сліди злочинів (різноманітні зміни, які вносяться ними в навколишню обстановку); особа злочинця (комплекс властивостей злочинця, його зв'язків і відносин, пов'язаних з учиненням злочинів, що можуть бути використані для їх розслідування); особа потерпілого (характер поведінки, майнове положення, соціальні зв'язки тощо)» [63, с. 9].

Зокрема, В. Ю. Шепітько вважає, що «…структура криміналістичної характеристики злочинів передбачає наявність певних елементів. Основними елементами криміналістичної характеристики є сукупності ознак, що визначають: 1) спосіб злочину; 2) місце та обстановку; 3) час вчинення злочину; 4) знаряддя і засоби; 5) предмет злочинного посягання; 6) особу потерпілого (жертви); 7) особу злочинця; 8) типові сліди злочину» [61, с. 274]. А ще одна група дослідників під керівництвом Є. В. Пряхіна визначила, що основними її складовими будуть наступні: «…1) типовий спосіб готування, вчинення та приховання злочину; 2) типова особа злочинця; 3) типова особа потерпілого; 4) типові час, місце, обстановка злочину; 5) типові знаряддя та засоби; 6) типовий предмет посягання; 7) типова слідова картина злочину» [60, с. 507]. Як бачимо, кількість елементів криміналістичної характеристики та їх формулювання майже не відрізняється.

Наостанок приведемо позицію А. Ф. Волобуєва, який зауважив, що «…криміналістична характеристика розкрадань майна повинна відбивати традиційні елементи їх механізму але з урахуванням тієї специфіки, яку накладає на них підприємницька діяльність, а також взаємні зв'язки з іншими злочинами, оскільки вони утворюють єдину технологію злочинної діяльності: особливості предмета посягання (матеріальні цінності, грошові

кошти, цінні папери); обстановка вчинення злочину (загальноекономічні і правові умови підприємницької діяльності, організаційно-правові форми підприємств, стан контролю з боку відповідних державних органів, місце знаходження суб'єктів підприємництва та існування між ними певних відносин тощо); способи підготовки, вчинення і приховування розкрадання (прийоми створення сприятливих умов для заволодіння майном, прийоми безпосереднього заволодіння майном та його використання, заходи щодо маскування розкрадання, вчинення супутніх розкраданню злочинів); сліди розкрадання (документів та речових доказів, свідчень осіб, що вказують на протиправне заволодіння майном); особливості суб'єкта розкрадання та супутніх злочинів (підприємця-фізичної особи, посадових осіб і службовців юридичної особи - суб'єкта підприємництва); особливості потерпілого від розкрадання (підприємця, окремих громадян)» [11, с. 35].

З приводу дотичних досліджень до нашого, то, для прикладу, С. В. Самойлов вказував на наявність в системі криміналістичної характеристики шахрайств, учинених із використанням мережі «Інтернет», таких складових як: «…1) предмет посягання; 2) спосіб учинення злочину; 3) обстановка вчинення злочину; 4) характеристика особи злочинця; 5) характеристика особи потерпілого; 6) відомості про типові сліди злочину». Автор встановив, що «…у 98 % випадків учинення шахрайств із використанням мережі «Інтернет» предметом посягання є гроші юридичних або фізичних осіб, як у готівковій так і в безготівковій формі» [128, с. 17].

Наразі А. В. Рейнгольд виокремлював в структурі криміналістичної характеристики шахрайства в інтернет-комерції наступні елементи: «…спосіб вчинення шахрайства; слідова картина; особа шахрая; особа потерпілого; місце, час та обстановка в розрізі законодавчого регулювання комерційних правовідносин у мережі Інтернет» [114, с. 76]. А вже Т. В. Коршикова виділила в криміналістичній характеристиці шахрайств, учинених з використанням електронно-обчислювальної техніки, такі складові: «…предмет злочинного посягання; способи шахрайств, учинених з

використанням електронно-обчислювальної техніки; слідова картина; обстановка шахрайств, учинених з використанням електронно-обчислювальної техніки; особа злочинця; особа потерпілого від шахрайств, учинених з використанням електронно-обчислювальної техніки» [56, с. 82].

Досить вдалою вважаємо структуру криміналістичної характеристики, наведеної І. О. Коваленком відносно шахрайства в сфері банківських електронних платежів, який вирізнив в ній такі елементи: спосіб учинення шахрайства; обстановка вчинення кримінального правопорушення; слідова картина; особа шахрая; особа потерпілого [38, с. 124].

На основі опрацювання матеріалів кримінальних проваджень та аналізу вищенаведених досліджень науковців, нами в структурі криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу виділено наступні складові:

– спосіб підготовки, безпосереднього вчинення та приховування шахрайства;

– обстановка вчинення шахрайства у сфері використання інтернет-банкінгу;

– слідова картина протиправного діяння;

– особа шахрая;

– особа потерпілого [101, с. 234].

Констатуючи вищенаведене, зазначимо, що підтримується позиція групи вчених-криміналістів, які вказують на беззаперечну обов’язковість дослідження криміналістичної характеристики. Зауважено, що реальне значення досліджуваної наукової категорії в можливості її практичного використання під час розслідування шахрайства у сфері використання інтернет-банкінгу. Зазначено, що криміналістичну характеристику в кримінальних провадженнях досліджуваної категорії можна застосовувати для висунення відповідних версій та під час проведення окремих СРД на будь-якому етапі розслідування. Надано авторське визначення криміналістичної характеристики як сформованої на основі судово-слідчої

практики і досліджень науковців з різних юридичних галузей сукупності інформаційних даних про криміналістично значимі властивості та ознаки конкретного кримінального правопорушення (виду, групи), які мають сталі кореляційні зв’язки, а також що має на меті допомогу в попередженні й розслідуванні окремих категорій протиправних діянь. Виділено наповнення структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу.

1.3. Особливості основних елементів криміналістичної характеристики

Системоутворююче місце у структурі криміналістичної характеристики, на нашу думку, займає спосіб учинення кримінального правопорушення. З огляду на зазначене, серед складових вказаної наукової категорії спочатку охарактеризуємо саме його.

Ми підтримуємо позицію А. Е. Жиліна, який доречно зауважив, що «…кожен елемент криміналістичної характеристики має своє індивідуальне значення для структури в цілому та побудови кореляційних зв’язків зокрема. Практичне значення вказаної категорії полягає у допомозі уповноваженим особам, які беруть участь у розслідуванні окремих протиправних діянь, шляхом використанню відомостей, що визначені нами як ознаки та властивості окремих її елементів. Вказаною інформацією можливо скористатися при проведенні окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів. Крім того, її необхідно застосовувати під час побудови версій та аргументації відповідних слідчих ситуацій. Тобто дослідження та надання відповідної характеристики кожному елементу криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів має значення для корегування початкового етапу кримінального провадження» [23, с. 89].

З приводу сутності вказаного елементу, В. А. Журавель констатує, що «…потрібно застосовувати функціональний аспект поведінки злочинця для характеристики способу вчинення злочину як системи дій, прийомів, операцій, що спрямовані на досягнення певного злочинного результату. Знання типових способів вчинення злочинів дозволяє ефективно застосовувати одну з найбільш ефективних та практичних схем розслідування їх, яка представляється науковцями у послідовності: від слідів злочину – до способу його вчинення; від способу вчинення – до особи злочинця» [26, с. 28].

Ґрунтуючись на аналізі судово-слідчої практики та дослідженнях науковців (А. Е. Жилін [25], Т. В. Коршикова [51], В. Р. Мойсик [85], Н. В. Павлова [93], А. В. Рейнгольд [117]) нами встановлено, що ключовим елементом криміналістичної характеристики є спосіб учинення шахрайства, який у 100 % випадків мав повноструктурний характер. Це зумовлено обов’язковою наявністю етапів підготовки та приховування протиправного діяння.

Крім того, ми вважаємо за потрібне визначити чинники, які впливають на обрання способів протиправних дій у сфері використання інтернет-банкінгу. Серед них нами виокремлено такі як бажання матеріального збагачення шахраїв, довірливість потерпілих від шахрайських дій та розвиток ЕОТ.

Повертаючись до розгляду способу вчинення кримінального правопорушення як структурного елементу криміналістичної характеристики вбачаємо обов’язковим звернення до С. М. Зав’ялова, який зауважував, що вказана складова виявляється як сукупність способів підготовки, безпосереднього вчинення та приховування його результатів. Також науковець-криміналіст вказує, що «…ними виступає різновид діяльності людини, якій притаманні соціально-психологічні якості, орієнтувальні, сенсомоторні особливості суб’єкта» [27, с. 5].

Зокрема, В. В. Тіщенко в структурі способів вчинення протиправного

діяння визначає «…комплекс діянь злочинця з підготовки, вчинення і приховування злочину, обумовлених метою злочинного діяння, властивостями особи злочинця й обстановкою (об'єктивними і суб'єктивними факторами), результати яких відбиваються на матеріальних та інтелектуальних слідах, що характеризують психічні й фізичні риси особи злочинця» [150, с. 18]. Як бачимо, дослідники визначали спосіб вчинення кримінального правопорушення в поєднанні окремих його елементів: підготовки, безпосереднього вчинення та приховування результатів.

Відтак, найперше ми будемо розглядати спосіб підготовки до вчинення шахрайства. З цього приводу, К. Д. Заяць говорить про те, що «…шахрайства даної форми мають високий рівень латентності. Типові схеми обману розраховані на використання юридичної безграмотності, низькі інтелектуальні здібності більшості людей, а також схильності людей до навіювання з боку сторонніх осіб. Активно використовуються шахраями і хворобливі стани окремих представників суспільства такі, як ігроманія, алкоголізм, наркоманія, патологічна любовна залежність. Зазначені фактори обумовлюють три основні причини відмови потерпілих від звернення до правоохоронних органів із заявами про вчинення кримінальних правопорушень. По-перше, більшість навіть не розуміють, що стали жертвами схеми обману. По-друге, значна частина потерпілих вважають себе винуватими у тому, що були введені в оману, і не бажають виявляти свої негативні риси (жадібність, наївність, довірливість тощо). По-третє, потерпілі самі належать до групи потенційних кримінальних елементів, які займаються крадіжками, незаконними операціями з наркотичними засобами чи іншими злочинними діями» [32, с. 207].

Наразі І. О. Коваленко, ґрунтуючись на аналізі опитування працівників правоохоронних органів, встановив, що «…мали місце такі підготовчі заходи до вчинення шахрайства у сфері банківських електронних платежів: підготовка відповідної електронно-обчислювальної техніки (комп'ютер, ноутбук, планшет тощо); створення програмного забезпечення для вчинення

окремих видів шахрайства; вибір об’єкта, що буде предметом шахрайських дій; вибір кола осіб, які стануть жертвами шахрайських дій» [39, с. 138].

С. С. Сисолятін, наприклад, визначив такий «…перелік підготовчих дій до вчинення кримінальних правопорушень, пов’язаних з використанням інтернет-банкінгу: 1) підбір та підготовка необхідної електронно-обчислювальної техніки (комп’ютерів, ноутбуків, планшетів); 2) створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту; 3) несанкціоновані збут або розповсюдження через мережу Інтернет інформації з обмеженим доступом, яка зберігається в комп’ютерах; 4) створення повідомлень електрозв’язку для подальшого їх масового розповсюдження, здійснене без попередньої згоди адресатів; 5) створення сприятливих умов для здійснення злочинних дій та ін.» [132, с. 152].

Наразі А. І. Кунтій серед заходів підготовки до вчинення кримінальних правопорушень в сфері ЕОТ визначив наступні: «…1) підбір знарядь та програмного забезпечення для вчинення злочину; 2) вибір об’єкта, стосовно якого буде вчинено злочин; 3) підбір співучасників і розподіл ролей; 4) установлення спостереження за об’єктом, вивчення режиму роботи чи розпорядку дня; 5) вибір місця зберігання викраденої інформації; 6) підшукування зацікавлених в інформації осіб (юридичних осіб)» [60, с. 867].

Зокрема, окрема група вчених-криміналістів (А. Е. Жилін, К. О. Чаплинський, М. М. Єфімов) на основі аналізу анкетування респондентів зробили висновок, що «…мали місце наступні підготовчі дії до вчинення шахрайства досліджуваного виду: підбір та підготовка певної електронно-обчислювальної техніки (ноутбук, комп’ютер, планшет тощо) – 88 %; розробка програмного забезпечення, необхідного для вчинення окремих видів шахрайства (фішинг, кардінг) – 81 %; вибір об’єкта шахрайських дій – 100 %; вибір кола осіб, стосовно яких будуть вчинені шахрайські дії – 92 %» [21, с. 45].

Аналіз матеріалів судово-слідчої практики [Додаток Б] дозволив вивчення матеріалів кримінальних проваджень з'ясувати підготовчі заходи щодо вчинення шахрайства, а саме:

– підбір необхідної ЕОТ (комп'ютер, смартфон, ноутбук) – 94 %;

– підготовка спам-ботів для їх застосування під час використання е-банкінгу потерпілими – 19 %;

– створення відповідного програмного забезпечення (вірусних програм) – 8 %;

– підбір групи осіб, стосовно яких буде вчинено шахрайські дії, – 87 %;

– підготовка необхідної обстановки для вчинення шахрайських дій – 69 %;

– підбір співучасників для здійснення шахрайських дій – 34 %;

– розподіл ролей між ними – 28 %.

Наступним елементом, який ми розглянемо, буде спосіб безпосереднього вчинення шахрайства у сфері використання інтернет-банкінгу. Наприклад, С. В. Самойлов запропонував «…класифікувати способи вчинення досліджуваних шахрайств за наступними підставами: а) шахрайства, які пов'язані із купівлею/продажем у мережі «Інтернет»; б) шахрайства, сутність яких полягає в отриманні коштів (майна) шляхом надсилання листів чи повідомлень; в) шахрайства, які для заволодіння коштами (майном) потребують розробки та розміщення в мережі «Інтернет» дублікатів або вузькоспеціалізованих сайтів для надання псевдопослуг; г) шахрайства, які спрямовані на отримання персональних (реєстраційних) даних (так званий «фішинг»); д) шахрайства, пов'язані з обігом електронних грошей; є) шахрайства, для вчинення яких використовується спеціалізоване та/чи шкідливе програмне забезпечення; е) «комбіновані способи» шахрайств» [127, с. 4].

Для прикладу, наведемо наступну ситуацію: гр. А. на початку листопада 2021 р. з метою власного збагачення вирішив організувати незаконну схему шахрайського заволодіння грошовими коштами, шляхом

незаконних операцій із використанням ЕОТ відносно фіктивного продажу товарів в мережі Інтернет за допомогою створених ним оголошень на веб-сайті «olx.ua». З метою реалізації свого протиправного умислу, спрямованого на заволодіння чужими грошовими коштами, шахрай із використанням ЕОТ (власного ноутбука з програмним забезпеченням встановлених інтернет-браузерів, які надають доступ до всесвітньої мережі інтернет) власноручно створив облікові записи на веб-сайті «olx.ua»де розмістив ряд оголошень про продаж неіснуючих товарів, а саме радіаторів для опалення, парогенераторів, бочок «Єврокуб», крісел коконів, прасок, дров, генераторів та інших товарів, не маючи наміру виконувати вказані послуги. У подальшому, 16 листопада 2021 року близько 16 год. 00 хв., шахрай під час листування через додаток «Viber», із використанням вказаного ноутбука з метою власного збагачення ввів в оману потерпілого гр. П., повідомивши недостовірні дані щодо отримання останнім радіатора для опалення, після оплати завдатку за товар та надав реквізити банківської картки АТ «Правекс Банк» до якої мав доступ та на яку необхідно здійснити перерахування грошових коштів в сумі 600 грн. в якості оплати завдатку за придбане майно» [146].

Раціональною також вбачаємо позицію С. С. Чернявського, який вказав, що «…дослідження способів учинення шахрайств шляхом незаконних операцій з використанням ЕОТ виступає своєрідним «ключем» до описання інших значущих елементів криміналістичної характеристики» [157, с. 9]. Зі свого боку, О. А. Самойленко сформулювала типові способи вчинення протиправних діянь у кіберпросторі, як-от: «…1. Способи злочинних дій, пов’язані з функціонуванням соціально-орієнтованих мереж (від англ. social networks), діяльність яких заснована на так званій вікі(viki)-технології. 2. Способи злочинних дій, пов’язані з функціонуванням технології BitTorrent, створеної для передавання великих за обсягом файлів одним користувачем іншому або громадськості. 3. Способи злочинних дій, пов’язані з функціонуванням сервісів електронної дошки оголошень (від англ. абревіатури «ВВС»). 4. Способи злочинних дій,

пов’язані з функціонуванням технологій електронної комерції, створені для здійснення торгівлі через Інтернет. 5. Способи злочинних дій, пов’язані з функціонуванням технології електронної розсилки (e-mail, від англ. electronic mail); IP-телефонії (найчастіше через комп’ютерну програму Viber; програмне забезпечення із закритим кодом Skype), призначені для відправлення/отримання електронних повідомлень між користувачами комп’ютерної/телекомунікаційної мережі. 6. Способи злочинних дій, пов’язані з функціонуванням технологій електронних платіжних систем (англ. electronic payment systems), призначені для здійснення платіжних операцій через мережу Інтернет. 7. Способи злочинних дій, пов’язані з функціонуванням технології зберігання та обробки інформації. 8. Способи злочинних дій, пов’язані з функціонуванням шкідливого програмного забезпечення. (з англ. «crimeware», де «crime – злочинність, software – програмне забезпечення; часто як синонім застосовують «вірус»)» [124, с. 140-156].

На основі вивчення матеріалів кримінальних проваджень [Додаток Б] нами було визначено найбільш типові способи безпосереднього вчинення шахрайства, зокрема: фішинг, спамінг і кардинг.

Отже/таким чином, вважаємо за доцільне привести твердження Т. В. Коршикової, яка засвідчила, що існує такий «…вид фішингу як смішинг (англ. SmiShing) – шахрайство за допомогою SMS-повідомлень. У цьому випадку посилання на підроблений сайт відправляється через SMS, або шахраї просять надіслати їм необхідну інформацію про банківську карту у відповідному повідомленні. Схожий на фішинг існує такий спосіб шахрайства як фарминг (англ. Farming, від слова «farm» – «ферма»). Він виражається в перенаправленні клієнта на помилкову адресу за допомогою шкідливої програми. Жертва обману вводить в пошуковий рядок адреси сайту свого банку, але дана програма відправляє його на підроблений шахрайський сайт. Різновидами фішингу є: 1) фішингові сайти; 2) фішингові електронні листи; 3) фішингові SMS-повідомлення» [52, с. 131].

З приводу деяких приховування результатів протиправних дій досить вдалою вважаємо думку окремої групи науковців (В. К. Весельський, С. М. Зав'ялов, В. В. Пясковський), які виділили серед них такі як: «…1) способи приховування матеріальних слідів, що відбилися в навколишній обстановці внаслідок готування і вчинення злочину; 2) способи приховування предметів посягання та наслідків заволодіння ними, розпорядження і використання; 3) способи вживання заходів з маскування і фальсифікації слідів злочину; 4) способи вживання заходів з протидії розшуку злочинця; 5) способи вживання заходів з протидії щодо встановлення істини загалом» [9, с. 37].

Для прикладу, гр. Х. на початку лютого 2022 р. з метою власного збагачення вирішив організувати незаконну схему шахрайського заволодіння грошовими коштами, шляхом фіктивного продажу товарів в мережі Інтернет за допомогою створених ним оголошень на веб-сайті «olx.ua». З метою реалізації свого протиправного умислу шахрай за допомогою власного ноутбука марки «Asus» з програмним забезпеченням встановлених інтернет-браузерів, які надають доступ до всесвітньої мережі інтернет власноручно створив облікові записи на веб-сайті «olx.ua», де розмістив ряд оголошень про продаж неіснуючих товарів, а саме газових плит та інших товарів, не маючи наміру виконувати вказані послуги. У подальшому, 20.07.2022 р. гр. Х. під час листування через додаток «Viber», не маючи на меті надання послуги з продажу газової плити, ввів в оману гр. Й., повідомивши недостовірні дані щодо отримання останньою газової плити, після оплати завдатку за товар та надав реквізити банківської картки АТ «Комінбанк» на яку необхідно здійснити перерахування грошових коштів в сумі 1400 грн. в якості оплати завдатку за придбане майно [145]. Після встановлення гр. Х. та його затримання було проведено його допит в якості підозрюваного. Шахрай надавав завідомо неправдиві покази, але після пред'явлення йому речових доказів та матеріалів кримінального провадження пішов на співпрацю з уповноваженою особою.

Після вивчення матеріалів кримінальних проваджень [Додаток Б] нами було визначено такі способи приховування шахрайських дій у сфері використання інтернет-банкінгу, а саме:

– знищення ЕОТ, яку використовували під час учинення шахрайських дій, – 69 %;

– маскування вірусних програм під їх справжні аналоги – 32 %;

– відмова від надання показань – 58 %;

– використання VPN та інших засобів маскування місцезнаходження ЕОТ – 43 %;

– дача завідомо неправдивих показів (зокрема щодо неправдивого алібі) під час проведення процесуальних дій (допит, одночасний допит раніше допитаних осіб) – 31 %.

На підставі узагальнення наукових розробок учених (В. Б. Коба [34], О. Л. Мусієнко [87], В. В. Сисолятін [136], С. С. Чернявський [159]) встановлено, що з'ясування обстановки шахрайства дозволяє уповноваженим особам визначити подальші напрями розслідування, а також низку першочергових СРД, НСРД та невідкладних процесуальних і розшукових заходів.

Для початку, приведемо умовивід А. І. Анапольської, яка основними умовами, які допомагають вчинення шахрайств вказала наступні: «…відсутність практики постійної зміни паролів та кодів доступу до системи електронних розрахунків; відсутність між працівниками банку розмежування доступу до комп'ютерної інформації про електронні рахунки; надання комплекту комп'ютерної техніки у безконтрольне користування співробітникам; відсутність контролю за порядком проведення електронних розрахунків тощо» [2, с. 7].

Для прикладу, 06 серпня 2022 р. гр. Ю. за допомогою незаконних операцій з використанням ЕОТ за допомогою додатку «Viber», представившись волонтером на Я., умисно надав недостовірні відомості гр. О. про те, що він є волонтером та має змогу надати останній послугу, що

полягала у передачі грошових коштів рідним на тимчасово-окуповану територію Запорізької області. Після чого, 06.08.2022 об 11:11 год. шахрай в ході подальшого листування з потерпілою , під приводом передачі грошових коштів, отримав грошові кошти у сумі 4000 грн. з розрахункового рахунку АТ «Державний ощадний банк України» на ім'я потерпілої на ім'я гр. А., яка не будучи обізнаною про злочинний намір останнього, надала йому реквізити своєї онлайн-картки та дані для входу до інтернет-банкінгу. Продовжуючи реалізацію свого протиправного умислу, шахрай за допомогою інтернет-банкінгу здійснив вхід до мобільного додатку «NeoBank» та здійснив переказ грошових коштів на власну банківську карту [139]. Як бачимо, обстановка шахрайства визначається умовами часу й місця, які здебільшого не мають чітких територіальних і часових меж.

Також доцільною також вбачаємо позицію О. Л. Мусієнка, який стверджує, що «…при шахрайстві, місце його вчинення має особливе значення, оскільки є джерелом певних слідів, що відображають механізм злочинної дії, взаємини злочинця та жертви. При цьому … деякі шахрайські дії можуть реалізовуватися в декількох місцях, не пов'язаних між собою. Результати узагальнення та аналізу кримінальних справ про шахрайство, показують, що місцем вчинення шахрайства є місця купівлі-продажу предмету посягання – 31,7 %; вулиця – 16,4 %; вокзали – 15,3 %; посередницькі фірми – 15,1 %; агентства нерухомості – 11,3 %; місце проживання потерпілого – 10,2 %; місце проживання злочинця – 0,4 %» [86, с. 7].

А вже, І. О. Коваленко засвідчує, що «…обстановку вчинення шахрайства в сфері використання банківських електронних платежів слід розглядати як у фізичному сенсі, із врахуванням місця знаходження комп'ютерно-технічного устаткування, з якого здійснювалися шахрайські дії, так і як віртуальний простір, в якому передавалася та зчитується цифрова інформація» [36, с. 386]. З огляду на зазначене, з'ясовано, що обстановка має специфічний характер і характеризується такими ознаками: а) шахрайські дії

відбуваються у віртуальному просторі; б) злочинні дії можуть відбуватися як у різних регіонах держави, так і за її межами; в) шахрайські дії не мають чітко визначеного місця події.

До того ж, проаналізовано систему інформаційних даних щодо обстановки шахрайства у сфері використання інтернет-банкінгу на основі опрацювання просторово-часових, економічних, психологічних і соціальних факторів.

З приводу місця безпосереднього вчинення шахрайства, то, для прикладу, А. С. Білоусов зауважує, що воно «…і місце, де наступають наслідки злочину і де вони можуть бути виявлені, можуть перебувати на досить таки великій відстані одне від одного, наприклад, в різних приміщеннях однієї організації, в різних містах однієї країни і навіть в різних країнах чи й континентах» [6, с. 9].

Зокрема, С. В. Самойлов серед місць вчинення шахрайства в мережі Інтернет виокремлює наступні: «…місцезнаходження банкоматів (магазин, вулиця тощо); місцезнаходження 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); місцезнаходження установ, де впроваджено системи розрахунків за допомогою пластикових кредитних карток» [126, с. 93].

На основі вивчення матеріалів кримінальних проваджень [Додаток Б] нами було встановлено найбільш поширені місця вчинення шахрайських дій, а саме:

– місця розташування ЕОТ, що були використані під час учинення шахрайства (місце проживання або роботи підозрюваного, місця загального доступу) – 76 %;

– місця розміщення терміналів, банків, банкоматів та інших фінансових установ – 15 %;

– місця перебування особи потерпілого, на яку були спрямовані

шахрайські дії, – 28 %.

Стосовно слідової картини то, для прикладу, Х. І. Духа наголошує тому, що вона «…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» [16, с. 263].

Наприклад, окрема група дослідників (Р. Л. Степанюк, С. І. Перлін) вказала на те, що «…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» [148, с. 288].

Досить вдалим вбачаємо твердження Т. В. Коршикової, яка зауважила, що «…специфіка механізму утворення інформаційних слідів визначається кіберпростором, тобто слідоутворюючим об'єктом, яким виступає програмно-технічний засіб, а слідосприймаючим об'єктом – комп'ютерною інформацією. Існує порядок зчитування інформації з її носія, а саме: фізичні сигнали (фізичний рівень) – цифрова форма (логічний рівень) – текст, графіка, звук (семантичний рівень); під час запису інформації на її носій – у зворотному напрямі. Зміни на будь-якому рівні, що відбуваються У результаті відповідного впливу (фізичний – за допомогою технічних пристроїв; програмний без участі людини; вплив людини на зміст інформації

за допомогою програмних засобів) відразу ж призводять до змін на інших рівнях. На слідосприймаючому об’єкті відображається не форма слідоутворюючого об'єкта, а їх властивості, оскільки програмно-технічні засоби не мають зовнішньої форми» [50, с. 53].

А вже А. І. Анапольська зазначила, що «…типові сліди злочинів, вчинених у сфері функціонування електронних розрахунків, можуть бути розподілені на: матеріальні сліди (сліди-відображення, сліди-речовини, сліди-предмети), ідеальні та електронні цифрові сліди. Кількість слідів, їх види та місця виявлення прямо залежать і можуть змінюватися залежно від обраного злочинцем способу готування, вчинення та приховування злочину. В окрему групу виділені електронні-цифрові сліди, під якими слід розуміти відомості (повідомлення, дані), зафіксовані на матеріальному носії та об'єктивно представлені у вигляді відображення інформації тимчасового та ідентифікаційного характеру в автоматизованих інформаційних системах, що утворюється за допомогою електромагнітної взаємодії, пов’язаної з подією злочину» [3, с. 165].

Наразі А. В. Рейнгольд на основі аналізу судово-слідчої практики та опитування респондентів у провадженнях стосовно шахрайства в інтернет-комерції зробив висновок, що «…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» [120, с. 75].

На основі опрацювання матеріалів кримінальних проваджень було визначено сукупність даних стосовно матеріальних та особистісних слідів, а

також виокремлено серед них особливу групу слідів, характерну для вчинення шахрайства у сфері використання інтернет-банкінгу – цифрових (електронних, віртуальних) слідів. Тобто доведено, що слідову картину шахрайства становлять три групи слідів – матеріальні, ідеальні та цифрові сліди. Остання група слідів була наявна в 100 % вивчених кримінальних проваджень [Додаток Б]. Як бачимо, особливу роль у слідовій картині відіграють цифрові (електронні, віртуальні) сліди, які здебільшого виявляють у таких місцях:

а) профілях соціальних мереж (Facebook, Instagram, Twiter);

б) месенджерах (Telegram, Viber);

в) застосунках для переписок криптовалютного спрямування (Binance, OKX);

г) кеш-пам’яті онлайн магазинів;

д) базах інтернет-провайдерів тощо.

Також слід наголосити на кореляційних зв’язках між способами шахрайських дій і слідами їх застосування.

Стосовно значення особа правопорушника як одного з елементів криміналістичної характеристики, то ми повністю поділяємо твердження В. В. Сисолятіна, який зазначив, що вказана складова є однією з основних майже всіх сучасних методиках розслідування. Автор пояснив це наступними акторами: «…По-перше, вказаний елемент має чітко виражені кореляційні зв’язки з іншими складовими досліджуваної наукової категорії. А по-друге, він в будь-якому випадку має місце в криміналістичній характеристиці, адже без його встановлення не буде повним склад кримінального правопорушення. Тому вважаємо за необхідне здійснити криміналістичний аналіз особи, яка вчиняє протиправні діяння, пов’язані з використанням інтернет-банкінгу» [133, с. 31].

Зі свого боку, О. В. Бородай вказує на те, що «…відомості про особу злочинця як елементу криміналістичної характеристики злочинів дають слідчому можливість скласти уявлення про певну групу осіб, до якої може

належати злочинець, а виділення типових рис кіберзлочинців допомагає оптимізувати процес їх виявлення й проведення розслідування» [7, с. 217].

Доречною вбачаємо думку окремої групи науковців (В. І. Курило, О. Є. Михайлов, О. С. Яра) які вказують, що «…кримінологічний аспект вивчення особи злочинця припускає різні «рівні» узагальнення цього поняття: конкретна особа, різні категорії злочинців, загальне поняття злочинця і містить у собі вивчення всіх зовнішніх і внутрішніх обставин, що сформували її як особу. У цьому плані кримінологічний аспект найбільш широкий і містить у собі як кримінально-правовий, так і процесуальний моменти» [68, с. 85-86].

Наразі О. Р. Лужецька формулює її як «…типову модель особистості людини, яка вчинила злочин, з притаманними їй біологічними, психологічними і соціальними властивостями, ознаками, що беруть участь у процесі детермінації механізму злочину, зумовлюють особливості його відбивних можливостей та процесу слідоутворення і разом з тим відчувають на собі й відображають вплив інших осіб, предметів і процесів, що взаємодіють з ними» [74, с. 200].

А вже К. Д. Заяць зауважує, що «…шахраїв, які користуються механізмом ринкових відносин і які вміють прикривати злочин порушеннями умов укладеної угоди та, відповідно, переводити претензії потерпілих на рівень спорів у судах, необхідно назвати «елітою» серед представників кримінального світу. Злочинці даної категорії – це інтелектуально обдаровані особи, які бачать метою свого життя виявляти слабкості державної системи й законодавства, та користуватися ними для власного збагачення» [29, с. 12].

Ми підтримуємо позицію А. В. Рейнгольда, який надав наступну «…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» [115, с. 189].

Зокрема, Ю. Ф. Іванов та О. М. Джужа наводять такі групи відомостей, що розкривають особу злочинця, як-от: «…1) соціально-демографічні; 2) кримінально-правові; 3) моральні якості; 4) психологічні ознаки; 5) фізичні (біологічні) характеристики» [33, с. 86-87].

Цікавою є позиція Л. В. Лефтерова, який відмічає, що «…кібершахрайство – особлива категорія злочину, яка змінила поняття та деякі принципи обману та зловживання довірою. Так, сучасний кібершахрай може бути таким, у якого відсутні акторські здібності, він взагалі може не показувати свою поведінку, в нього можуть бути нерозвинені навички й уміння вербального спілкування. З огляду на те, що провідне місце серед стійких психологічних особливостей особистості займають мотиви шахраям, як і кібершахраям, властиві прагнення до самоствердження на соціально-психологічному рівні (пов'язано з потребою домогтися визнання з боку найближчого оточення – сім'ї, друзів, знайомих, колег по роботі) і на індивідуальному рівні (пов'язано з бажанням підвищити самооцінку і посилити самоповагу шляхом здійснення вчинків, що сприяють, на думку особистості, подоланню будь-яких психологічних слабкостей). Не менш типовими для кібершахраїв є ігрові мотиви, властиві особам, які скоюють злочини не тільки і не стільки з метою отримання матеріальної вигоди, а скільки заради гри та ризику, для отримання гострих відчуттів. Досить яскраво ці мотиви виявляються в ситуаціях, в яких здійснюється інтелектуальне протиборство і змагання в спритності, де потрібні кмітливість, уміння максимально використовувати сприятливі обставини і швидко приймати рішення» [70, с. 67].

А вже І. М. Даньшин демонструє те, що «…особа злочинця включає низку елементів, тобто певну кількість різних ознак, властивостей, рис, особливостей, які об'єднує так: соціально-демографічні ознаки (відомості про стать, вік, рівень освіти, рід занять, стаж роботи, сімейний стан, місце проживання, інші дані про соціальний статус особи). Соціально-демографічні

ознаки дають істотну інформацію про особу злочинців, що може бути використана як із науковою, так і прикладною метою, зокрема під час розробки та реалізації заходів запобігання злочинам; особистісно-рольові властивості (соціальні позиції, рольові особливості тощо); соціально-психологічні якості (особливості особи, які сформувалися на базі її психічних станів і процесів у ході власного соціального досвіду; спрямованість особистості, мотиваційна сфера, потреби, установки, інтереси тощо); риси правової й моральної свідомості; кримінально-правові ознаки (спрямованість злочинної поведінки суб'єкта на конкретні суспільні відносини, узяті під охорону законом; ступінь і характер суспільної небезпечності вчиненого злочину; способи, обрані для досягнення злочинної мети; мотив, яким керувався суб'єкт злочину; ставлення винного до вчиненого)» [66, с. 39].

Вважаємо вірною думку М. О. Малія, який зауважував, що «…особа комп'ютерного злочинця – це фізична особа (людина), яка вчиняє кримінальні правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), різного рівня новітніх комп'ютерних засобів і технологій (нанокомп'ютери, портативні комп'ютери, суперкомп'ютери, квантові комп'ютери тощо) та різного виду засобів (електронного, біологічного або нейробіологічного електронного інтелекту тощо), електронних банків даних, систем та комп'ютерних мереж, або інших засобів комп'ютерної інформатизації та різного роду інформаційно-телекомунікаційного обладнання (державного, приватного, наземного, космічного)» [77, с. 67-68].

Також доцільним вбачаємо твердження В. В. Логінової, яка акцентувала увагу на тому, що особу злочинця слід оцінити за такими групами критеріїв як: «…1) біографічні дані: прізвище, ім'я, по-батькові; дата та місце народження; національність, громадянство, місце проживання, освіта, спеціальність, стаж роботи; сімейний стан, склад родини; попередня судимість; 2) дані про матеріальний стан: загальний дохід і житлові умови сім'ї (для неповнолітніх) тощо; відомості про стан здоров'я й психологічні

особливості: загальний стан здоров'я; фізичні вади; наявність стійкої хвороби, групи інвалідності; дані про характер, темперамент, вольові та емоційні властивості; 3) суспільно-виробнича характеристика: термін роботи або навчання в певному місці; ставлення до такої діяльності, товаришів по роботі (навчанню); участь у громадському житті; наявність дисциплінарних або громадських стягнень та заохочень; 4) суспільно-політична характеристика: членство у політичній партії, молодіжній, громадській організації; участь у виборчих кампаніях, збройних конфліктах; наявність нагород та почесних звань; 5) суспільно-побутова характеристика: взаємовідносини в родині; спосіб життя й коло знайомих; вживання алкоголю; відносини із сусідами; участь у громадській роботі за місцем проживання; наявність адміністративних або громадських стягнень; 6) ставлення до скоєного та поведінка в ході слідства; ціннісні орієнтири особистості; мотиви та мета скоєння злочину; наявність сп'яніння при вчиненні злочину тощо» [72, с. 116-118].

На підставі аналізу судово-слідчої практики [Додаток Б] було встановлено, що шахрайські дії здебільшого вчиняють особи чоловічої статі (74 %). Щодо вікових особливостей встановлено, що в 7 % випадків кримінальні правопорушення здійснюються особами віком від 16 до 20 років, 20–30 років – 34 %, 30–40 – 31 %, 40–50 років – 20 %, 50 років і старші – 6 %. Таким чином, найбільш криміногенна група – це особи віком від 20 до 40 років.

Наразі Л. М. Прудка, опрацьовуючи окремі аспекти вказаної групи ознак злочинця, відмічає, що «…у шахрайських посяганнях на перший план виступає яскраво виражений корисливий мотив. Проте, окрім користі, мотивами шахрайської діяльності можуть бути: самоствердження, приховане прагнення до влади. Залежно від домінування того або іншого мотиву у разі скоєння злочину, зазначає вчена, уявляється можливим поділити шахраїв, що використовують маніпуляцію свідомістю і поведінкою жертв, на такі групи: 1) шахраї з провідним корисливим мотивом, раціональним підходом

до способу вчинення шахрайства, підготовкою до його вчинення і усвідомленням усіх наслідків злочинної діяльності; 2) шахраї з провідним ігровим мотивом (шахрай – гедоніст, що отримує задоволення від процесу злочинної діяльності); 3) шахраї з ведучим ситуативно виниклим мотивом, під впливом сприятливих (з точки зору реалізації злочинного задуму) обставин; 4) шахраї з провідним мотивом, що виник під впливом групового тиску» [110, с. 32].

З приводу рівня освіти шахраїв [Додаток Б] визначено наступні відомості: базову середню освіту має 2 % злочинців, середню – 3 %, середню спеціальну – 5 %, базову вищу – 27 %, вищу – 63 %.

Отже/наразі/зокрема, вважаємо доречним твердження О. І Миргородського, який зазначив, що можливо «…сформувати наступний кримінологічний портрет суб'єкта шахрайства, вчиненого у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки: громадянин України чоловічої статі у віці від 30 до 50 років, який має повну загальну середню освіту, раніше не судимий, на момент вчинення злочину визнаний працездатним, який офіційно не працює та не навчається. Акт делінквентної поведінки вчиняє одноособово, перебуває у тверезому стані. Нагадаємо, отримані результати дозволяють сформувати уніфікований портрет особи кримінального правопорушника, який вчиняє одне із наступних суспільно небезпечних діянь: 1) шахрайство, вчинене у великих розмірах; 2) шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки» [82, с. 131].

За результатами узагальнення даних кримінальних проваджень [Додаток Б] з'ясовано, що здебільшого шахраї не є місцевими жителями (92 %).

Підсумовуючи зазначене, було сформовано типовий «портрет» особи шахрая, ознаки якого мають важливе значення під час реалізації НСРД та розшукових заходів, а саме шахрайські дії у сфері використання інтернет-банкінгу в більшості скоюють особи чоловічої статі у віці від 20 до 40 років,

мають вищу освіту, неодружені, а також відрізняються досить високим рівнем інтелекту.

Крім того, слід зазначити, що досліджувані протиправні діяння в багатьох випадках (34 % опрацьованих кримінальних проваджень) вчиняються ОГ та ЗО. Тому вважаємо за необхідне також надати їх криміналістичні характеристику.

З приводу вказаного питання нами було опрацьовано ряд праць вчених-криміналістів, серед яких вважаємо за потрібне виділити таких як: К. О. Чаплинський [155, с. 5], А. М. Лазебний, Б. С. Левицький [69, с. 192], В. О. Луговий [73]. В той же час, одразу слід наголосити на тому, що, досить вірною у розрізі наповнення учасниками ОГ чи ЗО вважаємо позицію С. П. Мельниченка, який акцентував увагу, вона має наступний вигляд: «…1) лідер (організатор); 2) особи, що спеціалізуються на «придбанні» вогнепальної зброї, наприклад, викрадення (розбій, грабіж), купівлі на воєнізованих складах, у інших ОЗУ або у зоні АТО; 3) особи, які безпосередньо переміщують вогнепальну зброю (кур'єри - безпосередні виконавці, співвиконавці) до місця схованки або продажу (передачі); 4) особи, що здійснюють підготовку до вчинення злочину (придбання або виготовлення підробних документів, визначення шляхів та способів можливого переміщення вогнепальної зброї), підготовку транспортних засобів до перевезення тощо; 5) особи, що здійснюють збут вогнепальної зброї або забезпечують її зберігання (переховування)» [80, с. 82-83].

Стосовно формулювання терміну «організована злочинність», звернемось до Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» в ст. 1 якого визначено, що зазначена наукова категорія це «…сукупність кримінальних правопорушень, що вчиняються у зв'язку з створенням та діяльністю організованих злочинних угруповань» [109].

Підводячи підсумок, зазначимо, що проблематика розслідування діяльності ОГ та ЗО, які вчиняють шахрайства у сфері використання

інтернет-банкінгу, має важливе значення як в діяльності правоохоронних органів окремих держав, так і на міжнародному рівні в розрізі визначення нормативно-правової бази та рекомендацій щодо взаємодії окремих підрозділів різних країн [98, с. 200].

Найбільш точною вважаємо думку К. О. Чаплинського, який наголошував на обов'язковому існуванні у структурі ОГ чи ЗО таких учасників, як-от: «…лідери (організатори) організованих груп чи злочинних організацій; аналітичний блок (радники і консультанти); блок безпеки (розвідка і контррозвідка); блок прикриття (захисту), що складається із корумпованих чиновників і представників правоохоронних органів, а також з адвокатів, які обслуговують злочинні групи, та утримувача єдиної «каси»; активні члени: бойовики, безпосередні виконавці, охоронці, навідники та ін.» [156, с. 48-49].

На основі вказаних досліджень та опрацюванні матеріалів кримінальних проваджень [Додаток Б] за наведеною тематикою, нами запропоновано структуру злочинної організації, яка здійснює шахрайські дії у сфері використання інтернет-банкінгу, до якої входять такі групи осіб:

1) організатори;

2) адміністратори сайтів, де розміщують неправдиві відомості про товари або надання послуг;

3) продавці, які спілкуються з потенційними потерпілими (здебільшого через телефонні розмови або sms-переписки);

4) спамери (особи, які здійснюють розсилку листів стосовно інтернет-магазинів з продажу товарів або надання різноманітних послуг);

5) фішери (особи, які розсилають листи для отримання особистої інформації потенційних потерпілих);

6) програмісти (особи, які створюють спам-боти для розсилки та віруси для потенційних атак);

7) хакери (особи, які здійснюють вірусні атаки на об'єкти, що зацікавили злочинну організацію);

8) охоронці;

9) корумповані представники органів державної влади й управління, працівники правоохоронних органів, які беруть участь у прикритті організованої злочинної діяльності.

Стосовно особи потерпілого, для початку приведемо позицію В. Ю. Шепітько, який, на нашу думку, найбільш повно навів ряд її ознак та властивостей, як-от: «…відомості анкетного характеру (стать, вік, місце народження, роботи або навчання, стаж, професія (фах), сімейний стан, наявність родичів); соціально-психологічні дані (тип темпераменту, риси характеру, емоційні прояви, особливості взаємодії (спілкування) в колективі); особливості поведінки – до злочинної події, в момент вчинення злочину, після його вчинення; незалежні характеристики (за місцем роботи чи навчання, за місцем проживання, за показаннями рідних, близьких чи найближчого оточення); соціальні зв'язки (коло спілкування, найближчі знайомі, особливості проведення вільного часу, наявність або відсутність спільного бізнесу, комерційна діяльність, специфіка групової поведінки, бажання вступити в певні мікрогрупи); дані про суспільно-корисну діяльність, її особливості; матеріальне становище (наявність майна, в тому числі і нерухомості, грошових вкладів, джерело збагачення, наявність або відсутність боргових зобов'язань, отримання кредитів і можливість їх погашення); злочинний досвід (наявність або відсутність судимостей, зв'язки з кримінальними угрупованнями, дружні стосунки з особами, які притягувалися до кримінальної відповідальності); причини віктимної поведінки (виконання певних професійних функцій; соціальна деформація особистості) тощо» [168, с. 164-165].

А вже М. В. Сенаторов наступним чином визначив досліджувану категорію: «…потерпілий від злочину – це соціальний суб'єкт (фізична чи юридична особа, держава, інше соціальне утворення або ж суспільство в цілому), благу, праву чи інтересу якого, що знаходиться під охороною кримінального закону, злочином заподіюється шкода або створюється

загроза такої» [131, с. 60]

Зі свого боку, К. Л. Попов вірно зазначив, що «…особистість жертви шахрайства становить інтерес з точки зору її віктимного потенціалу стосовно вказаного протиправного діяння, в її соціально-психологічному дослідженні, окрім вже названих, можна визначити певні додаткові орієнтири. Серед вказаних орієнтирів слід виділити соціально-психологічні чинники зниження критичності та обачності особи, так як необачна поведінка властива переважній більшості жертв шахрайства. Тому необачність потрібно розглядати не лише як сутнісну (сталу) властивість особистості, але і як одну з ознак поведінки у конкретній ситуації, яка залежить, з одного боку, від соціального досвіду особи, її поінформованості, звичок, інших особистісних властивостей, а з іншого – від впливу елементів зовнішнього середовища, у якому потенційна жертва опиняється у конкретний момент часу [106, с. 169].

Досить цікаво С. В. Головкін вказав, що «…серед характерних ознак особи потерпілого за результатами дослідження встановлено: азарт (56,7 %), жадібність (33,5 %), ритуальні забобони (22,9 %), віра у щасливий випадок (21,8 %), особисті комплекси (17,3 %), лінь (12 %), неуважність (9,3 %), імпульсивність (8,6 %), підвищена самовпевненість (5,4 %), емоційна неврівноваженість (3,8 %). Поведінка потерпілого може проявлятися у різних проявах: від повної віктимності, уразливості до впливу шахрая, нейтрального ставлення до останнього або активної протидії йому. За даними нашого дослідження пік віктимності приходиться на 30-45 років, причому жінки складають переважну більшість – 66 % через властиву їм довірливість, підвищене почуття страху за близьких, забобонність, чоловіки відповідно – 34 %. На те, що жертвами потерпілі ставали саме в силу віктимологічних чинників, а не через власну неграмотність, свідчить рівень освіти потерпілих: 37 % з них мали вищу освіту, 22 % – середню, 29 % - середню спеціальну» [15, с. 190]. Як бачимо, автор охарактеризував особу потерпілого за окремими ознаками.

В свою чергу, А. Б. Мізерак вказав, що «…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» [84, с. 154]. В розрізі наведеної позиції вважаємо доцільним привести судження М. Ю. Литвинова, який відмітив, що «…потерпілими можна вважати й магазини електронної торгівлі в тих випадках, коли зловмисники використовували точну копію сайту реально існуючого магазину з метою отримання конфіденційної фінансової інформації про клієнтів магазину (наприклад, дані кредитних карт). В цьому випадку репутація магазину може постраждати. Наприклад, добре підготовлені в технічному плані шахраї, досконально вивчили механізми електронних угод, можуть зламати локальну мережу інтернет-магазину і скопіювати звідти все програмне забезпечення, включаючи бухгалтерські програми і списки імен і паролів. Після цього, увійшовши в Мережу, вони стають клонами цього магазину і можуть відслідковувати всі операції. Як тільки, нічого не підозрюючи, покупець здійснить покупку, до шахраїв потрапляє інформація про його кредитну картку. Після цього злочинець, використовуючи викрадене програмне забезпечення, списує з рахунку покупця гроші за покупку ще раз і переводить їх на рахунок магазину. Після цього, знову від імені магазину, оформляє повернення. Однак гроші повертати не законному власнику, а на рахунок шахрая» [71, с. 86].

Наостанок, приведемо позицію С. В. Чучка, який зазначає, що «…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.

Натомість, оцінити реальний відсоток потерпілих від таких шахрайств дуже складно, адже особи, яких ошукали, не завжди звертаються до правоохоронних органів. В основному причиною цьому є небажання таких осіб переживати довготривалу процедуру розслідування та невір'я у притягнення винних до кримінальної відповідальності через малу суму заподіяної шкоди. Хоча, мало потерпілих замислюються над тим, що у випадку наявності декількох епізодів загальна сума спричиненої шкоди від дій шахраїв поступово збільшується, і, за наявності доказової бази, можна притягнути винних до кримінальної відповідальності за значні збитки» [164, с. 353]. В той же час, ми вважаємо необхідним виокремити відповідні віктимогенні групи потерпілих від досліджуваної категорії протиправних діянь.

З приводу віктимогенних груп потерпілих від шахрайських дій у сфері використання інтернет-банкінгу вважаємо досить вірною думку І. О. Коваленка, який серед них виокремив наступні: «…а) особи, які піддалися впливу знайомих та родичів під час реалізації банківських електронних платежів; б) особи, які піддалися обману незнайомих осіб під час реалізації банківських електронних платежів; в) особи, які повідомили свої персональні дані працівникам банківської сфери; г) особи, які з огляду на негативні психічні стани піддалися впливу незнайомих осіб під час реалізації банківських електронних платежів» [43, с. 120].

На основі вказаних досліджень та опрацюванні матеріалів кримінальних проваджень [Додаток Б] за наведеною тематикою, нами запропоновано наступні віктимогенні групи потерпілих, зокрема:

а) особи, які через вплив родичів та знайомих повідомили їм свої ідентифікатори доступу до інтернет-банкінгу;

б) особи, які підлягли впливу незнайомих осіб та повідомили їм свої ідентифікатори доступу до інтернет-банкінгу;

в) особи, які повідомили власні ідентифікатори доступу до інтернет-банкінгу працівникам банківської сфери.

Констатуючи вищенаведене, відмітимо, що опрацювання ознак та властивостей вказаних елементів криміналістичної характеристики шахрайських дій у сфері використання інтернет-банкінгу, є її вагомою задачею для створення дієвої та ефективної вищевказаної наукової категорії.

Висновки до розділу 1

На основі опрацювання наукових основ формування методики розслідування шахрайства у сфері використання інтернет-банкінгу, слід надати такі висновки:

1. Через призму дослідження наукових праць вчених (О. А. Антонюк, А. Е. Жилін, І. О. Коваленко, Ю. М. Чорноус, А. В. Рейнгольд) проведено криміналістичний аналіз досліджуваної наукової категорії. З'ясовано сутність окремих наукових категорій, що характеризують правовідносини у сфері використання інтернет-банкінгу: «електронна торгівля», «інтернет-торгівля», «цифрова торгівля», е-банкінг», «інтернет-комерція», «інтернет-бізнес». Доведено, що вказані поняття відрізняються за змістом і наповненням. Наголошено, що методика розслідування окремих видів кримінальних правопорушень як розділ криміналістики почала досліджуватись приблизно у середині XX-го сторіччя. На початку її розвитку створювалися методики за загальнокримінальними протиправними діяннями – убивства, нанесення тілесних ушкоджень, крадіжки, грабежі, розбійні напади тощо. На межі XX-го та XXI-го сторіч розвиток інформаційних технологій та мережі Інтернет зумовив виникнення новітніх способів учинення кримінальних правопорушень, насамперед, шахрайств, злочинів у фінансовій сфері, а також виникненню нових складів протиправних діянь (наприклад, у сфері використання ЕОТ). Вказані фактори визначили необхідність побудови методики розслідування шахрайства у сфері використання інтернет-банкінгу як відносно «старого» складу кримінального

правопорушення у поєднанні з новітніми способами його вчинення.

2. За даними опитування працівників правоохоронних органів, більшість з них (95 %) вказали на необхідність формування окремої комплексної методики розслідування шахрайства у сфері використання інтернет-банкінгу. До основних факторів низької якості результатів розслідування респонденти віднесли наступні: непрофесійне процесуальне керівництво кримінальним провадженням – 49 %, низький професійний рівень працівників підрозділів правоохоронних органів, які беруть участь у розслідуванні шахрайства – 58 %, несвоєчасне проведення слідчих (розшукових) дій, НСРД та інших заходів – 41 %, неналежний рівень координації взаємодії уповноважених осіб з працівниками оперативних підрозділів, кіберполіції – 72 %, небажання свідків і потерпілих співпрацювати зі слідством – 27 % та ін. На основі узагальнення матеріалів судово-слідчої практики сформовано методику розслідування шахрайства у сфері використання інтернет-банкінгу з певними елементами, серед яких вагомими є наступні: а) сукупність тактичних операцій для реалізації конкретних завдань розслідування; б) профілактична діяльність уповноважених осіб у кримінальних провадженнях щодо шахрайств.

3. Здійснено аналіз криміналістичної характеристики та визначено її поняття, сутність та структуру. На підставі узагальнення наукових розробок (В. С. Кузьмічов, О. В. Одерій, Г. І. Прокопенко, Є. В. Пряхін, В. В. Тіщенко, А. П. Шеремет) встановлено, що криміналістична характеристика є відносно новою науковою категорією. Перші згадки про неї почалися у 60-70-их роках минулого сторіччя. З того ж часу постійно відбуваються наукові дискусії між різними науковцями з приводу як сутності та структури, так і загалом стосовно доцільності її входження в методику розслідування. Підтримується позиція вчених-криміналістів, які вказують на беззаперечну обов’язковість дослідження криміналістичної характеристики. Вирізнено такі складові криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу: типові способи шахрайства, обстановка кримінального

правопорушення, слідова картина, особа злочинця (шахрая), особа потерпілого (віктимогенні групи потерпілих). Доведено, що вказані елементи повинні бути максимально оптимізовані й спрямовані на вирішення тактичних завдань кримінального провадження. Надано власне авторське визначення криміналістичної характеристики кримінального правопорушення. Сформовано структуру вказаної наукової категорії.

4. Надано характеристику основним елементам визначеної криміналістичної категорії. На основі аналізу судово-слідчої практики та досліджень учених (А. Е. Жилін, Т. В. Коршикова, В. Р. Мойсик, Н. В. Павлова, А. В. Рейнгольд) встановлено, що центральним елементом криміналістичної характеристики є спосіб учинення шахрайства, який у 100 % випадків мав повноструктурний характер. Це пояснюється обов'язковою наявністю етапів підготовки та приховування протиправного діяння. Наголошено на чинниках, які впливають на обрання способів протиправних дій у сфері використання інтернет-банкінгу. З'ясовано підготовчі заходи до вчинення шахрайства, а саме: підбір необхідної ЕОТ (комп'ютер, смартфон, ноутбук) – 94 %; підготовка спам-ботів для їх застосування при використанні е-банкінгу потерпілими – 19 %; створення відповідного програмного забезпечення (вірусних програм) – 8 %; підбір групи осіб відносно яких будуть вчинені шахрайські дії – 87 %; підготовка необхідної обстановки для вчинення шахрайських дій – 69 %; підбір співучасників для здійснення шахрайських дій – 34 %; розподіл ролей між ними – 28 %. Надано характеристику типовим способам учинення шахрайства у сфері використання інтернет-банкінгу. Акцентовано на способах приховування шахрайських дій, серед яких виокремлено наступні: знищення ЕОТ, яка використовувалась під час вчинення шахрайських дій – 69 %, маскування вірусних програм під їх справжні аналоги – 32 %, відмова від надання показань – 58 %, використання VPN та інших засобів маскування місцезнаходження ЕОТ – 43 %, дача завідомо неправдивих показів (у тому, числі неправдивого алібі) при проведенні процесуальних дій (допит,

одночасний допит раніше допитаних осіб) – 31 %.

5. На підставі узагальнення наукових розробок вчених (В. Б. Коба, О. Л. Мусієнко, В. В. Сисолятін, С. С. Чернявський) встановлено, що з'ясування обстановки шахрайства дозволяє уповноваженим особам правильно визначитися з подальшими напрямами розслідування, а також окреслити низку першочергових СРД, НСРД та невідкладних процесуальних та розшукових заходів. З'ясовано, що обстановка має специфічний характер і характеризується такими ознаками: а) шахрайські дії відбуваються у віртуальному просторі; б) злочинні дії можуть відбуватися як у різних регіонах держави, так і за її межами; в) шахрайські дії не мають чітко визначеного місця події. Встановлено найбільш вірогідні місця учинення шахрайських дій.

6. Розглянуто слідову картину шахрайства. Визначено сукупність даних стосовно матеріальних та особистісних слідів, а також виокремлено серед них особливу групу слідів, характерну для вчинення шахрайства у сфері використання інтернет-банкінгу – цифрових (електронних, віртуальних) слідів. Аргументовано, що вказана група слідів має місце у 100 % вивчених кримінальних проваджень. Виокремлено кореляційні зв'язки між способами шахрайських дій та слідами їх застосування.

7. Значну увагу приділено особі злочинця (шахрая). Встановлено, що шахрайські дії здебільшого вчиняють особи чоловічої статі (74 %). Щодо вікових особливостей, встановлено, що у 7 % випадків кримінальні правопорушення здійснюються особами віком від 16 до 20 років, 20-30 років – 34 %, 30-40 – 31 %, 40-50 років – 20 %, 50 років і старше – 6 %. Як бачимо, найбільш криміногенна група – це особи у віці від 20 до 40 років. Стосовно критерію освіти, то більшість шахраїв має повну вищу (39 %) та базову вищу (34 %). Базова загальна середня освіта наявна у 2 % осіб, повна загальна – у 6 %, професійно-технічна – у 19 %. Здебільшого шахраї не є місцевими жителями (92 %). Сформовано типовий «портрет» особи шахрая, ознаки якого мають важливе значення під час реалізації НСРД та розшукових

заходів. Запропоновано структуру злочинної організації, яка здійснює шахрайські дії у сфері використання інтернет-банкінгу, до якої входять певні групи осіб. У випадках вчинення шахрайських дій у складі ОГ чи ЗО, то базову загальну, повну загальну та професійно-технічну освіту мали здебільшого особи, які реалізовували другорядні ролі.

8. Надано характеристику особі потерпілого. Виділено віктимогенні групи осіб відносно яких було вчинено шахрайські дії. Акцентовано увагу на кореляційних зв’язках особи шахрая з потерпілим.

Основні результати розділу опубліковано у працях [98; 99; 100; 101].

РОЗДІЛ 2
ПЛАНУВАННЯ ТА ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ ІНТЕРНЕТ-БАНКІНГУ

2.1. Аналіз та оцінка первинної інформації, а також коло обставин, що підлягають встановленню

Ми підтримуємо позицію І. О. Коваленка, який зазначив, що «…сфера здійснення безготівкових розрахунків є невід'ємною частиною економіки України. Розвиток і вдосконалення банківських електронних платежів зіграло важливу роль в банківській справі: дозволило знизити операційні банківські витрати, розширити сегмент активних клієнтів, підвищити їх лояльність. Але також гостро стоїть проблема інформаційної та фінансової безпеки клієнтів, що користуються дистанційними видами банківського обслуговування, зокрема при роботі з банківськими електронними платежами. Перед більшістю країн, в яких активно розвиваються операції з використанням онлайн банкінгу виникають різні види загроз шахрайства, не є винятком і Україна» [40, с. 98].

В розрізі зазначеного, вважаємо за необхідне привести позицію І. М. Попової, яка наголошує, що «…доцільно вирізнити такі, яким відповідає певна сукупність інформації, що її містять матеріали попередньої перевірки на стадії порушення кримінальної справи: 1) матеріали перевірки містять усі необхідні дані про обставини вчинення злочину і є достатніми для порушення кримінальної справи; 2) вихідні дані недостатні для порушення кримінальної справи, оскільки дають змогу припускати як наявність, так і відсутність події злочину (наприклад, виявлення факту зникнення керівників компанії-забудовника або зупинення будівництва без достатніх підстав), що потребує подальшого проведення цільових перевірочних заходів; 3) з

наявних даних убачаються ознаки об'єктивної сторони злочину, проте невідомі мотив, мета та суб'єкт (наприклад, виявлено факт укладання угоди щодо однієї квартири в новобудові з декількома інвесторами; виявлення ознак фіктивності в діяльності компанії-управителя коштів тощо); 4) матеріали не містять достатніх даних для порушення кримінальної справи та не можуть бути доповнені під час проведення додаткових перевірочних заходів або досудового слідства (наприклад, після знищення документів обліку діяльності будівельних організацій; відсутність можливості проведення документальних та інших перевірок тощо); 5) матеріали свідчать про відсутність складу злочину в діях службових осіб (бухгалтерська помилка, фінансова неспроможність унаслідок впливу чинників ризику, цивільно-правові відносини тощо)» [107, с. 118].

Згідно ч. 1 ст. 214 КПК України досудове розслідування розпочинається у випадках, коли: «Слідчий, дізнавач, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до Єдиного реєстру досудових розслідувань, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з Єдиного реєстру досудових розслідувань. Слідчий, який здійснюватиме досудове розслідування, визначається керівником органу досудового розслідування, а дізнавач - керівником органу дізнання, а в разі відсутності підрозділу дізнання - керівником органу досудового розслідування» [65].

В той же час, досить вдало Ю. П. Аленін вказав, що «…процесуальний порядок, встановлений у ст. 214 КПК України, не враховує загальні положення процесуальної діяльності та національні правові традиції. Оскільки будь-яка галузь процесуального права має передбачати попередній, перевірочний, фільтраційний етап перед основним провадженням» [1, с. 201].

Зі свого боку, А. Ф. Волобуєв сформулював такі підстави для внесення

первинного матеріалу в ЄРДР, як-от: «…1) заяви та повідомлення про кримінальне правопорушення, які надходять від фізичних або юридичних осіб і містять вказівку на окремі виявлені обставини (як правило, це повідомлення про очевидні злочини); 2) повідомлення про ознаки злочину, які надходять від оперативного підрозділу: відповідно до ч. 2 ст. 7 закону України «Про оперативно-розшукову діяльність» оперативний підрозділ, який здійснює оперативно-розшукову діяльність, у разі виявлення ознак злочину зобов'язаний невідкладно направляти зібрані матеріали для початку та здійснення досудового розслідування; у разі, якщо оперативно-розшукові заходи ще тривають, і їх припинення може негативно вплинути на результати кримінального провадження, підрозділ, який здійснює оперативно-розшукову діяльність, повинен повідомити відповідний орган досудового розслідування та прокурора про виявлення ознак злочину, закінчити проведення оперативно-розшукового заходу і лише після цього направити зібрані матеріали до відповідного органу досудового розслідування; 3) самостійне виявлення слідчим ознак злочину (наприклад, під час здійснення ним іншого кримінального провадження)» [63, с. 11-12].

Вважаємо за потрібне привести позицію К. Д. Зайця, який визначив, що «…типовими джерелами доказів у кримінальних провадженнях про шахрайства даної категорії можуть виступати: 1) показання потерпілого щодо обставин вчинення злочину; 2) показання свідків з числа осіб близького оточення потерпілого щодо обставин вчинення злочину; 3) зміст листування між шахраєм і потерпілим (дані вилучених скріншотів); 4) дані щодо одночасного листування шахрая з іншими потенційними жертвами; 5) квитанції про перерахування коштів потерпілим на рахунки шахрая; 6) квитанції про зняття з рахунків готівки, що потім передавалась шахраю; 7) кредитні договори та боргові розписки, що підтверджують факт отримання коштів потерпілим для розрахунків з шахраєм; 8) виписки по рахунках, що належать шахраю, про рух коштів по його банківським карткам; 9) факт користування підслідним сторінками в соціальних мережах від імені

вигаданих осіб; 10) факт впізнання потерпілим підслідного за ознаками голосу, якщо мали місце телефоні перемовини; 11) факт належності підслідному віш-карти, за допомогою якої здійснювались дзвінки потерпілому; 12) притягнення затриманого раніше до кримінальної відповідальності за вчинення аналогічних злочинів; 13) факт відсутності законних джерел прибутку у підслідного, при наявності в нього значних грошових коштів, джерело отримання яких він не може пояснити» [30, с. 76].

На основі аналізу судово-слідчої практики [Додаток Б] встановлено, що первинна інформація, що стала підставою для внесення відомостей в ЄРДР за фактом вчинення шахрайських дій [64] була одержана уповноваженими особами з наступних джерел:

а) заяви, листи та повідомлення, що надійшли від потерпілих від шахрайських дій – 67 %;

б) заяви, листи та повідомлення від громадян, які стали свідками вчинення шахрайських дій або одержали про них інформацію – 12 %;

в) звернення, заяви, листи та повідомлення від співробітників фінансових установ різних форм власності – 9 %;

г) матеріали справ, що було виокремлено з інших кримінальних проваджень – 3 %;

д) матеріали, одержані при реалізації НСРД або розшукових заходів – 7 %.

Для прикладу, приблизно з серпня 2021 р. гр. Й., який усвідомлюючи, що досягти мети незаконного збагачення шляхом вчинення протиправних дій в сфері ЕОТ він самостійно не зможе, розробив план злочинної діяльності, який у встановленому на цей час обсязі передбачав ряд заходів. Зокрема, створення закритих від загального доступу Telegram-каналів та ботів, як інструменту месенджера Telegram, який дозволяв би створення фішингових посилань, необхідних для заволодіння коштами. Також створення за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші

технічні та технологічні засоби і обладнання) фішингових посилань, зовні ідентичних послугам доставки інтернет-платформ безкоштовних оголошень «OLX» та «IZI.UA» - «OLX-доставка» та «IZI-доставка» відповідно, а також на сервісах BlaBlaCar та Нова Пошта, метою яких є отримання у довірливих або неуважних користувачів зазначених інтернет-платформ їх персональних даних та реквізитів платіжних карток. Крім того, наступним заходом було підшукання осіб, які у ЗО виконували б роль так званого «Кодера», до обов'язків якого у ЗО входило володіння технічними знаннями в сфері інформаційно-комунікаційних технологій, створення, за допомогою засобів електронних комунікацій та у подальшому підтримання роботи Telegram-боту. Наостанок серед заходів, які застосовував гр. Й. варто виокремити підшукання осіб, які у ЗО виконували б роль так званого «Вбівер», до обов'язків якого входило знання особливостей роботи міжнародних платіжних систем, автоматизованої банківської системи та який, маючи можливість відслідковувати у режимі он-лайн процес введення потерпілим за фішинговим посиланням [147]. Вказана шахрайська схема та її учасники були виявлені в ході відпрацювань працівниками управління протидії кіберзлочинам у м. Києві ДКП НП України та У подальшому визначені протиправні дії були внесені в ЄРДР.

В свою чергу, А. В. Рейнгольд вірно наголошував, що «…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» [119, с. 116].

З огляду на зазначене, нами запропоновано рекомендації щодо аналізу й оцінки первинної інформації, яка була приводом для початку

кримінального провадження, а саме надано алгоритм перевірочних дій та заходів, а саме:

– опрацювання відповідної заяви;

– за можливості проведення огляду місця події;

– відібрання пояснень від осіб, які володіють певною інформацією.

Вказаний алгоритм реалізується у досить короткі строки, адже до внесення відомостей в ЄРДР уповноважені особи мають лише 24 години. Виходячи з цього, важливого значення набуває невідкладне й ретельне проведення огляду місця події.

На основі аналізу наукових праць учених (І. О. Коваленко [42], Т. В. Коршикова [48], С. В. Чучко [163],) встановлено перелік слідчих версій, що слід висувати на первинному етапі розслідування шахрайства у сфері використання інтернет-банкінгу, а саме:

– про суб'єкта шахрайських дій;

– визначення напряму його пошуку;

– встановлення обставин шахрайських дій.

Крім того, під час вивчення опитування респондентів [Додаток А] нами було виокремлено тактичні помилки, які допускають уповноважені особи під час розслідування шахрайських дій, як-от:

– недотримання правильного порядку реалізації СРД, НСРД та інших розшукових заходів – 68 %;

– прорахунки в аналізі шахрайських дій на початковому етапі розслідування – 64 %;

– здійснення невідкладних СРД без участі відповідного спеціаліста – 61 %;

– неправильне визначення подальших напрямів кримінального провадження – 54 %;

– поверхневе проведення невідкладних СРД (огляд місця події, огляд ЕОТ) – 57 %.

Обставини, які підлягають встановленню під час розслідування

шахрайства у сфері використання інтернет-банкінгу, мають важливе значення для кримінального провадження з огляду на їх обов'язкове доведення до судового розгляду.

Для прикладу, в ч. 1 ст. 91 КПК України зазначено, що «…у кримінальному провадженні підлягають доказуванню: 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» [65].

В розрізі зазначеного стосовно визначення кола обставин нами було проаналізовано ряд праць дослідників, серед яких варто виокремити Ю. М. Чорноус [160], К. О. Чаплинського [154], В. В. Сисолятіна [135].

В свою чергу, окрема група науковців (М. М. Єфімов, І. В. Пиріг)

вказали, що обсяг обставин, які «…підлягають встановленню при розслідуванні кримінальних правопорушень, повинен визначатись виходячи з: предмета доказування (обставин, що підлягають встановленню); меж доказування у кримінальному провадженні, визначених у законі; ознак кримінального правопорушення, що розслідується, які мають місце в диспозиціях відповідних статей Кримінального кодексу; обставин, що визначаються своєрідністю кожного окремо взятого протиправного діяння» [20, с. 22].

Зі свого боку, С. І. Марко виокремив наступні типові обставини, що підлягають з'ясуванню в справах за фактом вчинення шахрайства, як-от: «…1) чи має подія злочинний характер, чи було вчинено шахрайство; 2) який механізм злочинної події; 3) у чому полягали дії злочинця; чи був обман або зловживання довірою з боку злочинця; 4) який спосіб обману або зловживання довірою був застосований; 5) де і коли вчинено шахрайство; 6) який період продовження шахрайських дій; 7) скільки часу минуло після вчинення злочину; 8) за яких обставин було вчинено шахрайство; 9) скільки було злочинців; 10) чи відбувся розподіл ролей серед шахраїв, у чому полягали функції кожного з них; 11) в якому напрямку і за яких обставин зникли злочинці; 12) які індивідуальні особливості майна, переданого злочинцям, який його характер і кількість; 13) чи був причинний зв'язок між обманом або зловживанням довірою та матеріальним збитком, заподіяним потерпілому; 14) чи були здійснені шахраєм підготовчі та супутні шахрайству дії; 15) які предмети або документи були залучені до злочинного діяння; 16) чи пред'являлися шахраєм які-небудь документи, їх характер і особливості, наявність реквізитів; 17) які сліди та речові докази могли бути залишені на місці злочину; 18) які предмети або документи були передані потерпілому; 19) хто є жертвою злочину, її психологічна та соціальна характеристика; 20) хто мав відомості про наявність у потерпілих цінностей; 21) коли і на підставі чого потерпілий запідозрив, що став жертвою злочину; 22) чому потерпілий передав майно шахраю; 23) хто міг знати і звідки могли

спостерігати те, що відбувається на місці злочину; 24) чи були аналогічні випадки в цьому чи інших регіонах України; 25) що сприяло вчиненню шахрайства» [60, с. 746-747].

Крім того, в розрізі предмету та завдань нашої дисертаційної роботи вважаємо досить доречним привести думку С. В. Чучка, який вказував на обов'язкове виокремлення окремих груп обставин, які мають бути встановлені під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет. Серед них автор виділив обставини, що стосуються події визначеного протиправного діяння, а саме різноманітні відомості про час, місце вчинення шахрайства, спосіб його вчинення, про знаряддя (засоби) протиправного діяння, про сліди шахрайства, про предмет злочинного посягання. Також дослідник вирізнив групу обставин, які характеризують особу потерпілого та злочинця, та причинкові обставини, які вказують на існування причинного зв'язку між діями винних осіб та їх наслідками. Наостанок науковець звернув увагу на таку групу як решта обставин, до якої заніс вид і розмір шкоди, завданої кримінальним правопорушенням, кваліфікуючі ознаки щодо розміру шкоди завданої злочином та інші [165, с. 95-96].

Підводячи підсумок, відмітимо, що в кримінальних провадженнях, розпочатих за фактом вчинення шахрайства у сфері використання інтернет-банкінгу, досить важливим є визначення обставин, які підлягають встановленню. Ми поділяємо позицію С. В. Чучка, який виокремив майже вичерпний їх перелік [97, с. 133]. Але в той же час вважаємо за доцільне більше конкретизувати обставини в досліджуваній категорії кримінальних проваджень, а саме:

1) обставини, що розкривають умови та способи вчинення шахрайства (інформація про час і місце його вчинення, відомості щодо способу підготовки, безпосереднього вчинення та приховування шахрайських дій, зокрема застосування спам-ботів, використання вірусних програм до ЕОТ потерпілих, використання різноманітних шахрайських схем), засоби, які

використовували під час учинення шахрайських дій;

2) обставини, які характеризують особу злочинця або групу осіб (кількість шахраїв, схема розподілу між ними обов'язків, визначення їхньої ролі в злочинному угрупованні);

3) обставини, які характеризують особу потерпілого (віктимність її дій, базовий чи професійний користувач ЕОТ);

4) причиново-наслідкові зв'язки між діями шахраїв і результатами, які їх характеризують;

5) встановлення причин та умов, що сприяли вчиненню шахрайських дій;

6) обставини, які обтяжують або пом'якшують покарання;

7) вид і розмір шкоди, яка завдана шахрайськими діями;

8) обставини, які є приводом для звільнення шахрая від кримінальної відповідальності.

2.2. Типові слідчі ситуації, що виникають під час розслідування шахрайства у сфері використання інтернет-банкінгу, та алгоритми їх вирішення

Розслідування кримінальних правопорушень повинно відбуватися в певній послідовності. Ця послідовність забезпечується проведенням СРД, НСРД та інших процесуальних дій відповідно до типових слідчих ситуацій. Вказана криміналістична категорія виконує роль регулятора реалізації вищеперерахованих заходів. Кримінальні провадження, розпочаті за фактом вчинення шахрайства у сфері використання інтернет-банкінгу, також потрібно здійснювати до зазначених ситуацій. Тому їх визначення та формулювання є важливим завданням для нашого дослідження. Крім того, необхідним є створення відповідних алгоритмів дій працівників правоохоронних органів для їх реалізації [105, с. 339].

Як вірно вказує В. В. Сисолятін «…алгоритмізація є обов'язковою складовою для будь-якого процесу, звичайно, лише в тих випадках, коли у його організатора на меті буде послідовна та цілеспрямована діяльність. Розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, не є виключенням. В той же час, алгоритмізація повинна бути побудована відповідно до певної системи. В цьому розрізі, процес розслідування будується на типових слідчих ситуаціях. Адже в собі вказані ситуації можуть акумулювати як криміналістичні версії, так і окремі відомості про подію протиправного діяння та її учасників (потерпілих, свідків, підозрюваних). Тому вважаємо необхідним дослідити типові слідчі ситуації при розслідуванні кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу» [134, с. 129].

Для початку приведемо тезу С. В. Самойлова, який зауважував, що «…на сучасному етапі розвитку суспільства інформатизація створює інноваційні різновиди злочинних дій, що надають можливість розширенню зони охоплення різних напрямів протиправної діяльності, зокрема шахрайств, що вчиняються з використанням ЕОТ. Недостатня обізнаність слідчих про різновиди типових слідчих ситуацій та відповідних їм слідчих версій призводить до погіршення ефективності початкового етапу розслідування, у зв'язку з невірним визначенням напрямів розслідування, вибору комплексу слідчих дій» [129, с. 25]. В розрізі вказаного, вважаємо актуальною думку В. Некрасова, який відмічав, «…кіберзлочинці відчувають себе вільно не тільки завдяки низькому рівню фінансової грамотності українців, а й вельми лояльному кримінальному законодавству. В Україні шахрай при першій судимості несе відповідальність у вигляді лише штрафу. Водночас навіть ліберальний ЄС рекомендує за кібершахрайство призначати перше покарання у вигляді позбавлення волі не менш, ніж на один рік. В Іспанії за це можна отримати 12 років, в Польщі – до 25 років, в США – три-чотири довічні терміни. В Україні у 2016 р. потрапили до в'язниці лише десять шахраїв» [89].

А вже інша група науковців (М. М. Єфімов, І. В. Пиріг) вказали, що «…структура кожної окремої методики розслідування містить певну кількість елементів, серед яких необхідно виділити типові слідчі ситуації. Усі кримінальні правопорушення розслідуються в конкретних умовах часу, місця, оточуючого середовища, взаємозв'язку з іншими процесами об'єктивної дійсності, поведінкою осіб, що виявилися втягнутими у сферу кримінального судочинства, та під впливом інших чинників, що залишаються невідомими для уповноваженої особи. Ця складна система взаємозв'язків утворює ту конкретну обстановку, в якій працює уповноважена особа та інші суб'єкти, що беруть участь у доказуванні розслідуваної події. Така обстановка одержала в криміналістиці загальну назву слідчої ситуації. Іншими словами, це існуюча на даний момент реальність, в умовах якої діє слідчий. Ситуацією в буквальному її значенні є сама реальність, яка виникає на певному етапі розслідування. Формування слідчої ситуації залежить від таких компонентів: психологічного характеру; інформаційного характеру; процесуального і тактичного характеру; матеріального й організаційно-технічного характеру. Поєднання усіх цих компонентів обумовлює індивідуальний характер кожної слідчої ситуації у кожен момент проведення розслідування. З таким визначенням даного поняття пов'язана можливість типізувати слідчі ситуації. Слідча ситуація – це сукупність умов, що об'єктивно складаються в процесі розслідування злочинів, утворюють своєрідну обстановку на його певний момент, яка ставить перед слідчим проблему вибору відповідного напрямку подальших дій і прийняття тактичних рішень [20, с. 23-24]. В розрізі зазначеного, вважаємо за потрібне привести тезу Є. В. Пряхіна, який відмітив те, що «…схема слідчих дій на різних етапах розслідування нерозривно пов'язана зі слідчою ситуацією, яка склалася, тобто з тим обсягом інформації про подію, яку в певний момент часу доводиться оцінити уповноваженій особі щодо перспективи розслідування» [57, с. 241].

В свою чергу, О. В. Лускатов формулював типову слідчу ситуацію як

«…сукупність даних про подію злочину та обстановку його розслідування на конкретному етапі, що впливає на вибір, черговість і тактику слідчих (розшукових) дій та здійснення інших заходів» [58, с. 347]. Інша група науковців (Р. І. Благута, О. М. Дуфенок, Б. В. Щур) звертає увагу на те, що «…слідчі ситуації з часом після проведення комплексу слідчих дій та оперативно-розшукових заходів можуть перейти з однієї категорії в іншу. Наприклад, початкова несприятлива слідча ситуація (відсутня особа злочинця) є типовою для багатьох видів злочинів, повідомлення про які надходять до районного відділу міліції. Одначе після ефективно організованої дослідчої перевірки, а також після проведення первинних слідчих дій таланить установити особу злочинця. Затриманий вини у вчиненні суспільно небезпечного діяння не визнає (виникає проміжна конфліктна слідча ситуація). У ході досудового слідства проведено інтенсивну роботу пошуку доказів, які підтверджують вину затриманого, і У результаті пред'явлення підозрюваному доказів він зізнається у вчиненні злочину і виявляє бажання сприяти провадженню слідства та встановленню істини у справі, компенсувати шкоду, завдану потерпілому (виникає кінцева сприятлива безконфліктна слідча ситуація)» [57, с. 242]. Як бачимо, ряд вчених-криміналістів звертались до визначення сутності та поняття типової слідчої ситуації. На основі вищенаведених позицій спробуємо надати власне формулювання досліджуваної наукової категорії.

Отже, типова слідча ситуація – це система відомостей про протиправну подію та обстановку її розслідування, що позначається на підборі та черговості проведення СРД, НСРД й інших процесуальних дій для найбільш ефективної реалізації конкретного етапу кримінального провадження.

Стосовно класифікації типових слідчих ситуацій, то приведемо позицію групи науковців (К. О. Чаплинський, В. М. Плетенець, І. В. Пиріг), які на основі опрацювання криміналістичної літератури визначили такі їх види, як-от: «…1) після виявлення факту крадіжки не отримано інформації, що дозволяє розшукувати злочинця; 2) після виявлення факту крадіжки

отримано окрему інформацію, що дозволяє розшукувати винну особу; 3) після виявлення факту крадіжки наявна інформація про крадія, якого затримано на місці вчинення злочину або невдовзі після його вчинення». Також автори акцентували увагу на тому, що наведені ситуації розрізняються ступенем поінформованості стосовно особи злочинця, тому відповідно й комплекси процесуальних дій та інших заходів (алгоритми розслідування) будуть відрізнятись по кожній окремій ситуації [58, с. 348].

Відносно типових слідчих ситуацій під час розслідування шахрайства у сфері використання інтернет-банкінгу, то, для прикладу, В. Ю. Шепітько серед них виділяє наступні: «…1) є дані про подію злочину і особу злочинця; 2) злочинець затриманий відразу після вчинення злочину; є дані про подію злочину, 3) спосіб його вчинення, особа злочинця невідома; 4) є дані про подію злочину, але механізм вчинення шахрайства і особа злочинця невідомі». Крім того, науковець вказав, що визначені типові ситуації «…передбачають висунення і перевірку слідчих версій. Основою для цього можуть бути такі загальні типові припущення: шахрайство мало місце; вчинено інший злочин; надійшла неправдива заява і злочинного діяння взагалі не було. Якщо передбачається, що шахрайство мало місце, то можливе існування таких типових версій: заволодіння матеріальними цінностями чи грошима могло бути вчинено за допомогою підроблених документів (доручень, накладних, кредитових авізо, договорів, посвідчень тощо); заволодіння майном могло бути вчинено за допомогою легальних форм підприємницької діяльності чи використання фіктивних підприємств; заволодіння майном припускається вчиненим за допомогою «ляльок» (речових чи грошових), підміни товарів або грошових знаків; заволодіння грошима (іншими цінностями) передбачається вчиненим за допомогою азартних ігор; заволодіння майном припускається вчиненим групою шахраїв-гастролерів та ін. Залежно від ситуації і версії, що перевіряється, слідчий обирає найбільш доцільні слідчі дії та оперативно-розшукові заходи, визначає їх послідовність і відповідний комплекс» [62, с. 451].

Зі свого боку, С. І. Марко відмічав, що «…відповідно до загальних положень криміналістичної методики слідчі ситуації під час досудового розслідування шахрайств можна класифікувати за всіма основними теоретичними критеріями. Проте найбільш доцільним видається приділити увагу типовим сприятливим, несприятливим, конфліктним і неконфліктним слідчим ситуаціям, зважаючи на їхні основну інформативну сутність і вплив на початковий, подальший та завершальний етапи розслідування цього виду кримінальних правопорушень. Варіанти типової сприятливої слідчої ситуації: – Особа з'явилася до правоохоронних органів, зізналася у вчиненні злочину, продемонструвала механізм учинення шахрайства. Зібрані докази (сліди пальців рук, показання свідків, висновки експертиз тощо) підтверджують вину особи. – Особа звернулась до правоохоронних органів із повідомленням про вчинення щодо неї шахрайських дій. Потерпілий указує на конкретну особу злочинця, надає документи та інші докази, які підтверджують його показання. У результаті проведення початкових слідчих (розшукових) дій виявилось можливим затримати особу злочинця. Зібрані у кримінальному провадженні докази підтверджують вину підозрюваного, викривають багатоепізодність шахрайської діяльності» [60, с. 744].

Зокрема/наразі, Д. А. Птушкін на початковому етапі розслідування шахрайства, вчиненого щодо об'єктів нерухомого майна громадян, виокремив наступні ситуації: «…1) сприятлива ситуація: законний власник брав безпосередню участь у здійсненні правочину щодо купівлі-продажу нерухомості, але через певні обставини (наприклад, юридична необізнаність) став потерпілим. Злочинець встановлений, або є інформація про злочинців, їх кількість, механізм вчинення злочину, що дозволяє проводити розслідування у повному обсязі; 2) несприятлива ситуація: здійснення угоди відбувалося у присутності потерпілого, з його згоди, але останній в силу певних обставин не здатний був адекватно сприймати характер своїх дій (через алкогольну чи наркотичну залежність, похилий вік тощо) і не може надати інформацію про злочинців, механізм вчинення злочину тощо; 3) несприятлива ситуація:

шахраї діяли за генеральною довіреністю на право скоювати будь-які операції з квартирою, що виписав потерпілий, помиляючись у справжніх намірах осіб. Є певна інформація про злочинців, сліди, механізм вчинення злочину, але цього недостатньо для затримання шахраїв та проведення розслідування у повному обсязі» [111, с. 75-76].

А вже І. О. Коваленка визначив наступні ситуації початкового етапу розслідування шахрайства у сфері використання банківських електронних платежів, а саме: «…1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай відомий – 19 %; 2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %; 3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %; 4) вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %» [45, с. 102].

Доречною також вважаємо позицію С. В. Чучка, який сформулював наступні ситуації під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет, як-от: «…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 та особистісна доказова інформація, злочинець невідомий – 17 %; 4) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, відсутня достатня доказова інформація – 8 %» [166, с. 127].

На останок приведемо позицію Т. В. Коршикової, яка наголошує на існуванні двох типових слідчих ситуацій під час розслідування шахрайства з

використанням ЕОТ. Зокрема, авторка перша ситуацію формулює наступним чином: встановлено факт шахрайства з використанням ЕОТ, є первинна інформація про особу (групу осіб), які можуть бути причетні до вчинення цього кримінального правопорушення або особу злочинця встановлено чи є достатньо даних для її встановлення. З приводу другої типової слідчої ситуації, то дослідниця визначає її так: встановлено факт шахрайства з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї [54, с. 127].

На основі опрацювання судово-слідчої практики [Додаток Б], а також наведених позицій науковців, нами сформульовано типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу, зокрема:

1) вчинено шахрайські дії, наявна особистісна доказова база, злочинця (шахрая) встановлено – 27 %;

2) здійснено шахрайські дії, є особистісна доказова база, злочинця (шахрая) не встановлено – 52 %;

3) вчинено шахрайські дії, наявна особистісна та матеріальна доказова база, злочинця (шахрая) не встановлено – 16 %;

4) вчинено шахрайські дії, повністю відсутня доказова база – 5 %.

Отже, зазначимо, що кримінальні провадження, розпочаті за фактом вчинення шахрайства у сфері використання інтернет-банкінгу, потрібно здійснювати відповідно до типових слідчих ситуацій. Надано їх авторське визначення як системи відомостей про протиправну подію та обстановку її розслідування, що позначається на підборі та черговості проведення СРД, НСРД й інших процесуальних дій для найбільш ефективної реалізації конкретного етапу кримінального провадження. Сформульовано типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу.

З огляду на визначене, вважаємо за доцільне привести твердження К. Ю. Назаренко, яка зауважувала, що «…аналіз і оцінка слідчої ситуації мають істотне значення, тому що дозволяють: зорієнтуватися у всьому

різноманітті 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 і 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; вивести з версій слідства; спланувати початковий етап розслідування» [88, с. 82]

Наразі окрема група дослідників (Н. А Жерж, М. Є. Дирдін) вказала, що «…для вирішення визначених ситуацій працівники Національної поліції України зобов'язані реалізувати ряд заходів, які акумулюються в певному порядку. Окремі науковці алгоритм дій слідчого в розслідуванні насильницьких злочинів визначають наступним чином: аналіз наявної інформації; оцінка вихідної слідчої ситуації, висунення версій за фактичними та ймовірними обставинами подій; постановка тактичних завдань і планування розслідування; проведення окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та тактичних операцій по перевірці висунутих версій» [22, с. 118-119].

Ми повністю підтримуємо позицію А. В. Рейнгольда, який відмітив, що «…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» [118, с. 127-128]. Тобто комплекс СРД, НСРД та інших процесуальних дій під час вирішення першої типової слідчої ситуації розслідування шахрайства у сфері використання інтернет-банкінгу має наступний вигляд:

– допит потерпілого;

– огляд ЕОТ потерпілого (комп'ютеру, смартфону, планшету);

– встановлення особи шахрая;

– допит шахрая у статусі підозрюваного;

– обшук у приміщеннях, де живе або працює шахрай;

– вилучення ЕОТ, виявленої під час проведення обшуку (комп'ютер, смартфон, планшет, жорсткі диски);

– призначення експертиз [96, с. 146].

Для прикладу, з 20 липня 2020 року гр. А. перебував на строковій військовій службі у військовій частині. 23 грудня 2020 року гр. А. вибув на лікування у шпиталь. У період з 26 по 30 грудня 2020 року, ОСОБА_5 , перебуваючи у військовому шпиталі, у інфекційному відділенні, познайомився із військовослужбовцем гр. Д., який також перебував на лікуванні у тому ж відділенні. У спілкуванні гр. А. заручився довірою перед гр. Б. та у нього виник умисел на заволодіння грошовими коштами останнього в сумі 5000 грн.. Реалізовуючи його, шахрай під приводом необхідності скористатися мобільним телефоном гр. Д. заволодів належним

останньому телефоном з доступом до мобільних додатків. Окрім того, продовжуючи свій злочинний намір на заволодіння грошовими коштами гр. Д., повідомив йому, що повинен отримати грошові кошти від матері, однак власну банківську карту залишив у військовій частині та попросив банківську карту гр. В. з пін-кодом до неї, заволодівши таким чином і нею. У подальшому, 30 грудня 2020 року, гр. А., маючи безперешкодний доступ до мобільних додатків мобільного телефону гр. Д., за допомогою кредитного інтернет-банкінгу оформив кредит у ТОВ «Смартівей Юкрейн» на суму 600 грн, поставивши електронний підпис з одноразовим ідентифікатором потерпілого. Зокрема, 30 грудня 2020 року, о 18 год. 18 хв., він же за допомогою кредитного інтернет-банкінгу оформив кредит в ТОВ «Манівео швидка фінансова допомога» на суму 2000 грн.. Зазначені грошові кошти перерахував на банківську картку та здійснив купівлю продуктів в магазинах м. Полтава, користувався кур'єрськими послугами «Glovo» та мобільними інтернет-додатками на суму 2000 грн. Загалом, гр. А. заволодів грошовими коштами потерпілого на загальну суму 4750 грн. [144]. У подальшому шахрая ідентифікували шляхом проведення допитів потерпілих та огляду смартфону потерпілого, де були збережено усі операції інтернет-банкінгу.

Стосовно другої слідчої ситуації, одразу відмітимо, що особа шахрая невідома, тому варто розпочинати заходи з його встановлення та розшуку. Відносно розшуку злочинців, то ми повністю поділяємо позицію В. О. Малярової, яка визначила систематичне виконання наступних задача, зокрема: «…виявлення джерел інформації про ознаки шуканого злочинця; побудова гіпотетичної моделі злочинця (шуканої особи) та встановлення його належності до: – широкої сукупності (класу) осіб за загальними ознаками; – вузької сукупності (групи) осіб за окремими ознаками; встановлення обмеженої, кількісно визначеної групи осіб, що перевіряються; встановлення особи, що перевіряється, тобто особи, яка згідно обставинам кримінального провадження може бути шуканим злочинцем, та при необхідності отримання від неї зразків для експертизи, згідно ст. 245 КПК

України; ідентифікація конкретної особи; встановлення шуканого злочинця» [78, с. 131]. Тобто у другій слідчій ситуації варто проводити наступні заходи, як-от:

– допит потерпілого;

– огляд місця події з метою виявлення доказів, які допоможуть обмежити коло підозрюваних;

– огляд ЕОТ потерпілого (комп'ютеру, смартфону, планшету);

– тимчасовий доступ до речей і документів;

– огляд та долучення до справи відеозаписів, фотографій;

– розшук та встановлення особи шахрая;

– встановлення особи шахрая;

– аудіо-контроль особи шляхом встановлення технічних засобів в публічно недоступному місці (транспортному засобі, квартирі);

– візуальне спостереження за особою;

– негласне знаття інформації з транспортних телекомунікаційних мереж;

– призначення експертиз [96, с. 147].

Зокрема, Т. В. Коршикова доречно вказувала, що «…для перевірки слідчих версій, які можуть висуватися за результатами аналізу IP-адрес, за якими здійснювалось використанням ЕОТ з метою вчинення шахрайства: 1) для вчинення шахрайства використовувалась одна IP-адреса; 2) для вчинення шахрайства використовувалось декілька IP-адрес; 3) для вчинення шахрайства використовувались невстановлені IP-адреси» [47, с. 369]. Як бачимо, обов'язковим зазначається аналіз IP-адрес, за якими здійснювалось використанням ЕОТ з метою вчинення шахрайства, що характерно і для ефективного розслідування досліджуваної категорії кримінальних правопорушень.

А вже А. В. Рейнгольд наголошував, на тому, що «…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» [121, с. 131].

Також, як доречно зауважила Г. В. Захарова, «…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. У тому числі й збирати докази щодо неспроможності підозрюваної особи за тих обставин та умов, що відбувалися та існували виконати взяті зобов’язання» [28, с. 145].

Зі свого боку, Д. А. Птушкін відмічав, що у «…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)» [112, с. 65].

Для прикладу, в середині листопада 2016 року гр. О. вступив у попередню змову з гр. З. та вчинив ряд заволодінь чужим майном шляхом обману через незаконні операції з використанням ЕОТ. У вказаний час, шахрай зі своїм подільником, з використанням невстановленої комп'ютерної техніки шляхом реєстрації Інтернет-сайтів з відповідними назвами доменних імен створив ряд «фейкових» Інтернет магазинів, до яких відносяться: http://technobox.net.ua, http://mobilook.com.ua, http://technolab.in.ua, http://technomart.net.ua, http://supersmart.in.ua, http://mobiliti.net.ua, http://mobiland.net.ua, http://technoplaza.net.ua, http://evoshop.com.ua, http://mobilson.com.ua. Вказані «фейкові» Інтернет-магазини спеціалізувалися на реалізації мобільних телефонів. Оформлення сайтів, порядок їх функціонування, а також розміщення інформації з повним технічним описом товару не викликали у покупців сумнівів у реальності існування Інтернет-магазинів. Більше того, гр. О. разом зі своїм співучасником, з метою залучення якомога більшої кількості осіб, що зацікавляться розміщеним на Інтернет-сайтах товаром, у невстановлений досудовим розслідуванням час, виклав завідомо неправдиву інформацію про продаж мобільних телефонів торгових марок «Apple», «Xiaomi», «Meizu», «Samsung» та інших популярних виробників, зазначаючи при цьому значно нижчу вартість товару, що продається, ніж пропонують інші продавці. Також з метою підняття рейтингів та пошукової конкурентоспроможності (СЕО-показники), які б дозволили при будь-якому пошуковому запиті користувача мережі Інтернет щодо купівлі мобільних телефонів видавати його Інтернет-магазин серед перших для потенціальних покупців, гр. О. разом зі своїм

співучасником, використовував послуги Інтернет-майданчика «http://price.ua», який дозволяв видавати для потерпілих порівняльну з іншими Інтернет-магазинами інформацію та показував, що ціна товару в його Інтернет-магазині значно нижча, ніж в інших магазинах. У подальшому шахрай переводив у готівку сплачені клієнтами «фейкових» магазинів грошові кошти через мережу банкоматів, розташованих як на території м. Дніпро, так і в окремих районах і містах Дніпропетровської області. Під час користування банкоматами гр. О. з метою уникнення фіксації камер відео- та фотоспостереження, які розташовані в банкоматах та на прилеглих територіях, з метою подальшого унеможливлення ідентифікації своєї особи одягав на обличчя заздалегідь підготовлену маску. Заволодівши таким чином грошовими коштами потерпілих, шахраї розпоряджались ними на власний розсуд [137]. Під час/у процесі розслідування наведеного факту шахрайства у сфері використання інтернет-банкінгу уповноваженими особами було реалізовано майже весь комплекс процесуальних дій та заходів, визначених нами по другій типовій слідчій ситуації, як-от: починаючи допитом потерпілих, а закінчуючи проведенням аудіо-контролю гр. О. шляхом встановлення технічних засобів в публічно недоступному місці (в його транспортному засобі «Toyota Camry»), візуальним спостереженням за ним та негласним знаттям інформації з транспортних телекомунікаційних мереж. Завдяки максимально ефективному здійсненні всіх вказаних заходів особу було затримано, а У подальшому винесено обвинувальний вирок у вчиненні кримінального правопорушення, передбаченого ч. 3 ст. 190 КК України.

У третій ситуації вчинено шахрайські дії, наявна особистісна та матеріальна доказова база, але особу злочинця (шахрая) не встановлено. У вказаній ситуації характерного значення набирає виявлення та збір матеріальної доказової інформації шляхом проведення огляду та призначення відповідних експертиз із метою ідентифікації шахрая. Тобто у визначеній слідчій ситуації уповноваженим особам необхідно здійснити такі додаткові заходи:

– огляд ЕОТ (аналіз змісту файлів, журналу дзвінків на ґаджетах потерпілого, електронної пошти, web-браузерів);

– сукупність пошукових заходів, спрямованих на встановлення IP-адреси шахрая (зняття інформації з електронних інформаційних систем або її частини, встановлення місцезнаходження радіоелектронного засобу, візуальне спостереження за особою).

Наразі Т. В. Коршикова зауважувала, що «…під час розслідування шахрайств, учинених з використанням ЕОТ, особливий інтерес викликають контрверсії (версії захисту), оскільки вони є найменш дослідженими. Якщо слідчий не візьме до уваги можливе висунення контрверсій, вони створюють певні труднощі під час розслідування такого виду шахрайства, що обумовлює необхідність їх перевірки з метою всебічності та об'єктивності розслідування. Практичний досвід розслідування шахрайств, учинених з використанням ЕОТ, засвідчив що контрверсії можуть висуватися з приводу будь-яких обставин події кримінального правопорушення, зокрема: підозрюваний заявляє, що ЕОТ, яка фігурує як засіб вчинення шахрайства, не належить йому, а її користувачем є інша особа, яка йому лише уявно відома. Підозрюваний просто надавав ЕОТ іншій особі в оренду чи просто безоплатно для користування; електронно-обчислювальну техніку, яка фігурує як засіб вчинення шахрайства, підозрюваний придбав вже після вчинення кримінального правопорушення; підозрюваний не знав, що він вчиняє шахрайство, так як предмет посягання він хотів передати у майбутньому через деякий час. І цю обставину підозрюваний пов'язує з проблемою відправки предмету посягання чи відсутністю своєчасної поставки цього предмета з іншої країни; підозрюваний відводить собі другорядну роль під час вчинення шахрайства з використанням ЕОТ; виявлені при обшуках записи підозрюваний пояснює тим, що він самостійно вирішив підвищувати свій інтелектуальний рівень з метою більш поглибленого вивчення якого-небудь предмета (зазвичай таких, які вивчають у вищих навчальних закладах)» [51, с. 116-117].

А вже окрема група науковців вказувала, що під час розслідування кримінальних правопорушень проти банківської системи слід проводити ряд СРД, серед яких варто виокремити огляд місця події. Автори зазначили, що «…у цьому разі залучений спеціаліст-бухгалтер або економіст звертає увагу слідчого на фрагменти документів, де відображено важливу інформацію для слідства, а також спеціаліст допомагає правильно зафіксувати ці дані у протоколі. До того ж, спеціалісти допомагають слідчому обрати лише потрібні документи для розслідування із значної їх кількості. Слідчий разом зі спеціалістами при огляді документів має можливість оперативно отримати потрібну інформацію про показники виконання плану, стан обліку та звітності. Окрім того, після огляду спеціалісти допомагають слідчому сформулювати питання для проведення економічної експертизи» [149, с. 160–166].

Четверта ситуація є найскладнішою з огляду на те, що відсутня майже будь-яка доказова (орієнтуюча) інформація. За цієї ситуації працівники правоохоронних органів повинні докладно допитати заявника та визначити подальші напрями реалізації кримінального провадження.

Зокрема, К. Д. Заяць вказував на те, що «…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» [31, с. 156].

Для прикладу, 10.09.2020 р. приблизно о 18 годині 34 хвилин гр. П., маючи на меті заволодіти грошовими коштами гр. Л. шляхом вчинення шахрайських дій, перебуваючи за адресою м. Запоріжжя в кімнаті потерпілої, заздалегідь отримавши в наслідок зловживання довірою пароль та логін від мобільного додатку інтернет-банкінгу «Приват24», та скориставшись доброзичливими відносинами з потерпілою внаслідок яких остання довіряючи залишила шахрайку одну у кімнаті, остання взяла її мобільний телефон марки та за допомогою вказаного сервісу з банківського рахунку гр. Л. перерахувала грошові кошти в розмірі 1500 грн. на своє ім’я. Після цього, шахрайка віддала вищевказаний мобільний телефон, а грошовими коштами розпорядилась на власні побутові потреби. Аналогічні протиправні дії були ще неодноразово вчинені шахрайкою [141]. В ході розслідування, потерпіла навіть не озвучувала гр. П. в якості можливого злочинця, адже перебувала з нею у досить дружніх стосунках. В той же час, працівники кіберполіції наголосили на тому, що шахраєм може бути будь-хто, і лише після цього гр. Л. назвала дані шахрайки.

З приводу реалізації окремих СРД, то В. О. Яремчук вказував, що «…під час розслідування банківських злочинів доцільно проводити одночасний допит двох чи більше вже допитаних осіб. При цьому запрошений спеціаліст, використовуючи свої спеціальні знання, може ставити запитання допитуваним особам і роз’яснювати слідчому показання цих осіб. На нашу думку, спеціаліст під час розслідування таких кримінальних правопорушень, приймаючи участь у проведенні допиту може

ставити різні види запитань допитуваній особі, використовуючи свої спеціальні знання, залучені до допиту спеціалісти можуть заперечувати проти поставлених запитань учасниками кримінального провадження, що беруть участь у допиті при розслідуванні банківських злочинів» [170, с. 457].

Підводячи підсумок, зазначимо, що нами визначено комплекс процесуальних дій під час вирішення типових слідчих ситуацій розслідування досліджуваного протиправного діяння.

Висновки до розділу 2

Під час опрацювання окремих аспектів планування та організації розслідування шахрайства у сфері використання інтернет-банкінгу, нами було зроблено такі підсумки:

1. Виокремлено проблемні питання, які формуються при організації та плануванні розслідування шахрайства. На основі аналізу судово-слідчої практики встановлено, що первинна інформація, що стала підставою для внесення відомостей в ЄРДР була одержана уповноваженими особами з наступних джерел: а) заяви, листи та повідомлення, що надійшли від потерпілих від шахрайських дій – 67 %; б) заяви, листи та повідомлення від громадян, які стали свідками вчинення шахрайських дій або одержали про них інформацію – 14 %; в) звернення, заяви, листи та повідомлення від співробітників фінансових установ різних форм власності – 9 %; г) матеріали справ, що було виокремлено з інших кримінальних проваджень – 3 %; д) матеріали, одержані при реалізації НСРД або розшукових заходів – 7 %.

2. Запропоновано рекомендації щодо аналізу й оцінки первинної інформації, яка була приводом для початку кримінального провадження. Надано алгоритм перевірочних дій та заходів, а саме: опрацювання відповідної заяви; за можливості проведення огляду місця події; відібрання пояснень від осіб, які володіють певною інформацією. Вказаний алгоритм реалізується у

досить короткі строки, адже до внесення відомостей в ЄРДР уповноважені особи мають лише 24 години. Виходячи з цього, важливого значення набуває невідкладне й ретельне проведення огляду місця події. На основі аналізу наукових праць учених (І. О. Коваленко, Т. В. Коршикова, С. В. Чучко) встановлено перелік слідчих версій, що слід висувати на первинному етапі розслідування шахрайства у сфері використання інтернет-банкінгу.

3. Виокремлено тактичні помилки, які допускають уповноважені особи під час розслідування шахрайських дій, як-от: недотримання правильного порядку реалізації СРД, НСРД та інших розшукових заходів – 68 %, прорахунки в аналізі шахрайських дій на початковому етапі розслідування – 64 %, здійснення невідкладних СРД без участі відповідного спеціаліста – 61 %, неправильне визначення подальших напрямів кримінального провадження – 54 %, поверхневе проведення невідкладних СРД (огляд місця події, огляд ЕОТ) – 57 %. Сформовано сукупність обставин, які необхідно встановлювати під час розслідування шахрайства у сфері використання інтернет-банкінгу.

4. На основі аналізу наукових праць вчених (О. М. Дуфенюк, М. М. Єфімов, В. А. Некрасов, І. В. Пиріг, Б. В. Щур) встановлено, що розслідування кримінальних правопорушень повинно відбуватися у певній послідовності. Ця послідовність забезпечується проведенням СРД, НСРД та інших процесуальних дій відповідно до типових слідчих ситуацій. Вказана криміналістична категорія виконує роль регулятора реалізації наведених заходів.

5. Зроблено висновок, що кримінальні провадження, розпочаті за фактом учинення шахрайства у сфері використання інтернет-банкінгу, потрібно здійснювати до вказаних ситуацій. Крім того, необхідним є створення відповідних алгоритмів дій працівників правоохоронних органів для їх реалізації.

6. Виокремлено типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу *відповідно до яких сформовано*

алгоритми дій уповноважених осіб.

7. Вказано, що комплекс СРД, НСРД та інших процесуальних дій під час вирішення першої типової слідчої ситуації розслідування шахрайства складається з таких заходів: допит потерпілого; огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета); встановлення особи шахрая; допит шахрая у статусі підозрюваного; обшук у місці проживання або роботи шахрая; вилучення ЕОТ, виявленої під час проведення обшуку (комп'ютер, смартфон, планшет, жорсткі диски); призначення експертизи.

8. Стосовно другої слідчої ситуації зауважено, що для її реалізації варто проводити наступні заходи, як-от: допит потерпілого; огляд місця події з метою виявлення доказів, що дозволяють звузити коло підозрюваних; огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета); тимчасовий доступ до речей і документів; огляд та долучення до справи відеозаписів, фотографій; розшук і встановлення особи шахрая; аудіо-контроль особи шляхом встановлення технічних засобів в публічно недоступному місці (транспортний засіб, квартира); візуальне спостереження за особою; негласне знаття інформації з транспортних телекомунікаційних мереж; призначення експертизи.

9. Акцентовано увагу, що у третій слідчій ситуації уповноваженим особам необхідно здійснити такі додаткові заходи: огляд ЕОТ (аналіз змісту файлів, журналу дзвінків на ґаджетах потерпілого, електронної пошти, web-браузерів); сукупність пошукових заходів, спрямованих на встановлення IP-адреси шахрая (зняття інформації з електронних інформаційних систем або її частини, встановлення місцезнаходження радіоелектронного засобу, візуальне спостереження за особою). Зауважено, що четверта ситуація є найскладнішою з огляду на те, що відсутня майже будь-яка доказова (орієнтуюча) інформація. За цієї ситуації працівники правоохоронних органів повинні докладно допитати заявника та визначити подальші напрями реалізації кримінального провадження.

Основні результати розділу опубліковано у працях [96; 97; 105].

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО-ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОВЕДЕННЯ ПРОЦЕСУАЛЬНИХ ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ ІНТЕРНЕТ-БАНКІНГУ

3.1. Організація і тактика проведення процесуальних дій на початковому етапі розслідування шахрайства у сфері використання інтернет-банкінгу

Початковий етап розслідування має досить важливе значення для кримінального провадження в цілому з огляду на те, що від ефективності реалізації усіх можливих дій (СРД, НСРД, інших процесуальних та пошукових заходів), які повинні бути проведені під час нього, залежить кількість та якість отримання доказової інформації. Ведучи мову про шахрайство у сфері використання інтернет-банкінгу, вказані заходи не втрачають своєї актуальності. Оскільки у випадках неякісного збору первинних відомостей доказування означених протиправних дій майже унеможливлюється. Тобто якісне і ефективне проведення допиту потерпілих, огляду місця події, огляду ЕОТ та інших заходів як процесуального, так і пошукового характеру, забезпечить належний початок кримінального провадження [104, с. 234].

Зокрема, В. В. Сисолятін правильно зауважував, що «…на початковому етапі розслідування є досить багато слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій, а також розшукових заходів, які варто провести в будь-якому випадку. Звісно, корелюючи їх у відповідності до конкретного протиправного діяння, яке було вчинено. Зокрема, під час розслідування вбивства – це огляд трупа та його експертиза для встановлення обставин та механізму смерті особи; крадіжки – огляд місця події для

з’ясування механізму вчинення протиправного діяння та виявлення матеріальної доказової інформації; шахрайства – допит потерпілого для визначення способу його вчинення тощо. Під час розслідування кримінальних правопорушень, пов’язаних з використанням Інтернет-банкінгу, безумовно також наявні обов’язкові процесуальні дії, які необхідно реалізувати до внесення відомостей в ЄРДР та одразу після цього для забезпечення належної доказової бази» [174, с. 112].

Для початку приведемо твердження групи вчених-криміналістів (Б. Є. Лук’янчиков, Є. Д. Лук’янчиков, С. Ю. Петряєв), які стверджують, що «…особливого значення програми розслідування набувають для початкового етапу. Результативність першочергових слідчих (розшукових) дій, інших заходів створює передумови для всебічності, повноти і об’єктивності розслідування. Навпаки, зволікання з проведенням першочергових дій у кримінальному провадженні, невміння обирати належні, що випливають із слідчої ситуації призводить до того, що злочини довгий час залишаються нерозкритими, не всі факти злочинної діяльності встановлюються, не усі винні притягуються до відповідальності» [75, с. 201].

Наразі А. П. Шеремет вказав, що «…названий поділ процесу розслідування має суттєве методичне значення, оскільки кожний із виділених етапів має певну специфіку в обсягу і методах даної криміналістичної діяльності. Тому для здійснення найбільш успішного розслідування злочину на всіх його етапах і на стадії підготовки до нього в методиці розслідування розробляються прийоми і способи дій слідчого з урахуванням особливостей вказаних етапів. Відповідно в кожній методиці виділяються особливості розслідування на першочерговому, наступному і заключному етапах. На першочерговому етапі слідчий встановлює наявність ознак злочину в події, що вчинена, та приймає рішення щодо порушення або відмови в порушенні кримінальної справи. На цьому етапі проводяться першочергові невідкладні слідчі дії – визначаються напрями розслідування, здійснюється пошук злочинця за «гарячими слідами», будуються версії тощо» [169, с. 337].

А вже колектив авторів під керівництвом В. Ю. Шепітька відмічав, що «…на початковому етапі розслідування шахрайства дії слідчого визначаються залежно від характеру даних, які в нього є. У процесі розслідування повинні бути доведені такі обставини: подія шахрайства (час, місце, спосіб вчинення злочину та ін.); винність конкретної особи у шахрайстві і мотиви вчинення злочину; обставини, що впливають на ступінь і характер відповідальності обвинуваченого; характер і розміри шкоди, заподіяної шахрайством; обставини, що сприяли вчиненню шахрайства. Для перевірки версії про те, що шахрайства не було, необхідно встановити, чи мав заявник майно і цінності, на які він посилається як на предмет злочинного посягання, чи не міг він його розтратити. У такому разі необхідно детально опросити заявника про обставини передачі майна та його індивідуальні ознаки. У заявника доцільно з'ясувати, де і коли було придбано майно або цінності, хто знав про їх існування, яким чином відбувалася подія, за яких обставин, в якому місці, хто міг бачити передачу майна, хто перебував на місці вчинення злочину тощо. У разі підтвердження заяви потерпілого порушується кримінальна справа. Якщо з часу вчинення злочину минуло небагато часу, організується спостереження в місцях найбільш ймовірної появи злочинця. За кримінальними обліками органів внутрішніх справ перевіряється, чи є в них дані стосовно осіб, які мають властивості, притаманні шахраю, чи не зареєстровані нерозкриті шахрайства, що вчинені способом, аналогічним використаному підозрюваним» [62, с. 452].

Досить доречною також вважаємо думку Є. В. Пряхіна, який акцентував увагу на тому, що «…початковий етап розслідування залежить від слідчої ситуації, що склалася, проте загальна видова окрема методика розслідування шахрайств передбачає проведення на початковому етапі розслідування таких слідчих та інших дій: допит потерпілого, огляд місця події, огляд предметів і документів, допит свідків, проведення попередніх досліджень спеціалістів-криміналістів (дактилоскопічних, трасологічних тощо), проведення оперативно-розшукових заходів для розкриття злочину по

«гарячих слідах», затримання злочинця, пред'явлення предметів для впізнання, призначення судових експертиз речових доказів і матеріалів, вилучених із місця події» [60, с. 332].

В свою чергу, Т. А. Пазинич зауважує, що «…на початковому етапі розслідування для перевірки інформації про шахрайство необхідними є такі документи: 1) рапорт працівника оперативного підрозділу, який здійснював перевірку повідомлення про шахрайство; у ньому повинні міститися дані про: а) потерпілу сторону; б) особу злочинця (якщо його встановили); в) місце, час і використані засоби вчинення злочину; г) розмір заподіяної злочином матеріальної шкоди; ґ) свідків; д) використання викрадених об'єктів; 2) заява або повідомлення потерпілого (фізичної особи або представника юридичної особи) про факт вчинення розкрадання майна; 3) показання потерпілого про обставини виявлення розкрадання, можливий механізм його вчинення, причетних до цього осіб і розмір завданої шкоди; 4) показання осіб, яким відомі окремі обставини вчинення розкрадання; 5) оригінали або завірені в установленому законом порядку копії документів, що визначають організаційно-правовий статус підприємства, на якому здійснено викрадення коштів; 6) оригінали або копії документів, що визначають організаційно-правовий статус підприємства, працівники якого причетні до вчинення розкрадання; 7) оригінали або копії договорів про надання певних послуг (охорони, обслуговування банкоматів, забезпечення безпеки й захисту електронної бази даних тощо), виконання яких пов'язано з учиненням розкрадання; 8) оригінали або копії документів, які відображають проведення певних фінансових операцій з використанням комп'ютерних програм і мережі (данні банківських розрахунків); 9) оригінали документів, дійсність яких викликає сумніви і які можливо використовувалися як засіб учинення або приховування розкрадання; 10) матеріали спеціальних перевірок (акти документальної ревізії, внутрішньобанківських перевірок, висновки спеціалістів з питань використання електронних технологій тощо); 11) Документи щодо характеристики комп'ютерно-технічних засобів,

програмного забезпечення і порядку їх використання на підприємстві (інструкції з експлуатації» [63, с. 163-164].

А вже С. І. Марко говорить, що «…початковий етап розслідування залежить від слідчої ситуації, яка виникла, проте загальна видова окрема методика розслідування шахрайств передбачає проведення на початковому етапі розслідування таких слідчих (розшукових) та інших дій: внесення відомостей про кримінальне правопорушення до ЄРДР, допит потерпілого, огляд місця події, огляд речей і документів, допит свідків, проведення оперативно-розшукових заходів для розслідування злочину по «гарячих слідах», затримання злочинця, пред'явлення предметів для впізнання, призначення судових експертиз речових доказів та матеріалів, вилучених з місця події. На початковому етапі можуть бути вжиті заходи забезпечення кримінального провадження» [60, с. 747]. Як бачимо, перелік дій на початковому етапі в усіх науковців майже незмінний.

Для прикладу, протягом 2019 року гр. Ф. за місцем свого фактичного проживання самостійно зареєструвалась в соціальній мережі «Instagram», де створила обліковий запис «С.», та за допомогою комп'ютерної техніки, мобільного терміналу та підключення до Інтернет провайдеру «Sky Link» у всесвітній мережі Інтернет, на вказаному сайті розмістила оголошення з приводу продажу жіночого одягу. Так, 08.09.2019 р. гр. Ф. під час листування у вищевказаній соціальній мережі з потерпілою гр. Л., обговорили умови продажу жіночого одягу на загальну суму 1180 грн., при цьому шахрайка, не повідомляючи останній про свої істинні наміри, повідомила потерпілій про те що, їй необхідно перерахувати на картку оплату за одяг в сумі 1180 грн. Таким чином гр. Л. У результаті шахрайських дій гр. Ф. 08.09.2019 р. через термінал перерахувала грошові кошти в сумі 1180 грн.. Після чого шахрайка на власний розсуд розпорядилась грошовими коштами, отриманими нібито за проданий нею жіночий одяг, якого в дійсності не мала наміру продавати. Подібні події відбувалися ще неодноразово протягом 2019 року [142]. На початковому етапі розслідування шахрайства у сфері використання інтернет-

банкінгу (за приведеним випадком, який відповідає другій типовій слідчій ситуації) необхідно реалізувати наступні заходи:

– допит потерпілого;

– огляд ЕОТ потерпілого (комп'ютеру, смартфону, планшету);

– огляд та долучення до справи відеозаписів, фотографій;

– розшук та встановлення особи шахрая;

– аудіо-контроль особи шляхом встановлення технічних засобів в публічно недоступному місці (транспортному засобі, квартирі);

– візуальне спостереження за особою;

– негласне знаття інформації з транспортних телекомунікаційних мереж;

– призначення експертиз.

Зі свого боку, В. Ю. Шепітько акцентує увагу на тому, що в якості «…свідків допитують осіб, у розпорядженні яких перебувало майно, незаконно отримане шахраєм, інших осіб, які бачили чи мали контакт зі злочинцем до шахрайства або під час його вчинення. При допиті свідків необхідно з'ясувати обставини передачі майна, ознаки зовнішності злочинців, їх одяг, прикмети. Слід визначити, коли їх бачили, про що розмовляли; які дії вказували на те, що злочинці переслідували шахрайські цілі, та ін. При допиті потерпілого необхідно з'ясувати: коли і за яких умов шахрай вчинив обман чи зловживання довір'ям і заволодів майном; чому потерпілий опинився в цьому місці; чи був він один або з ким-небудь з числа своїх знайомих; чи були якісь особи разом з шахраєм; як вони поводили себе; який спосіб шахрайства був застосований злочинцем; які предмети чи документи передано шахраю; хто мав відомості про наявність у потерпілого майна; коли і на підставі чого він запідозрив, що став жертвою злочину; які індивідуальні особливості майна, переданого злочинцям; в якому напрямку і за яких обставин злочинці втекли, та ін. Цей перелік є приблизним і не охоплює усіх питань, які з'ясовуються при допиті потерпілого під час розслідування різних форм і видів шахрайства. З метою виявлення, фіксації і

вилучення слідів злочину та інших речових доказів, з'ясування обстановки події проводиться огляд місця події або огляд предметів чи документів» [62, с. 452-454]. Тобто відомості про особу шахрая можливо отримати від потерпілого або свідків (очевидців) з приводу усіх можливих обставин вчиненого шахрайства у сфері використання інтернет-банкінгу.

З приводу огляду ЕОТ ми підтримуємо позицію Т. А. Пазинич, яка вірно відмічає, що «…особливість механізму вчинення шахрайств цього різновиду обумовлює необхідність залучення допомоги спеціаліста у сфері комп'ютерних технологій уже на стадії початкової перевірки інформації про ці кримінальні правопорушення й ухвалення рішення про відкриття кримінального провадження» [63, с. 165].

В свою чергу, В. М. Варцаба зауважував, що «…специфіка огляду ЕОТ передбачає такі підстави: 1) комп'ютерна інформація є специфічним об'єктом пошуку; 2) обстеження ЕОТ та носіїв інформації може набувати самостійного значення; 3) не завжди наявна можливість у вилученні ЕОТ, окремих їх комплектуючих, щоб за допомогою інших дій зафіксувати і дослідити інформацію; 4) обстеження ЕОТ і її носіїв завжди передбачає необхідність запрошення відповідного спеціаліста (у галузі комп'ютерних технологій, комп'ютерних систем тощо); 5) ЕОТ набуває все більшого поширення, й існують різноманітні програми захисту та екстреного знищення інформації» [8, с. 76].

А вже М. В. Салтевський зазначав, що починаючи зовнішній огляд ЕОТ спеціалісту варто встановити склад ЕОТ, а саме: «…наявність системного блоку, монітора, клавіатури, принтера, модему, безперебійного джерела живлення та інших периферійних пристроїв. Якщо це ноутбук – визначення його розмірів. Одночасно встановлюється: тип корпусу, матеріал, з якого він виготовлений, його колір, номер ЕОТ, марка, назви, серія, номер, країна виробник, форма, колір ЕОТ» [123, с. 19].

Вдалою вважаємо також думку Т. В. Коршикової, яка відмітила обов'язковість встановлення наступних обставин під час огляду ЕОТ, як-от:

«…наявність, кількість і розташування роз'ємів й портів на корпусі для під'єднання зовнішніх пристроїв, а також наявність і види вмонтованих пристроїв, мережевих плат та пристроїв, наприклад, дисководу для гнучких дисків, дисководу для компакт-дисків, відеоплат тощо; встановлення та визначення інших пристроїв, які у подальшому також будуть підлягати огляду з подальшим проведенням їх огляду» [50, с. 52].

Крім того, нами було розкрито особливості тактики огляду, а саме визначено основні ділянки, на яких можуть бути виявлені сліди шахрайських дій. Також акцентовано увагу на тактиці огляду електронних відомостей, які перебувають або у відкритому доступі в мережі Інтернет, або на матеріальних носіях інформації чи різноманітних серверах для їх зберігання. Так само було зауважено, що під час огляду ЕОТ (ноутбук, смартфон, комп'ютер) об'єктом огляду може бути безпосередньо ЕОТ, так і відповідні носії інформації.

Запропоновано низку тактичних завдань, які уповноважені особи мають реалізувати в кримінальному провадженні, а також розроблено комплекси дій для їх вирішення в межах проведення початкового та подальшого етапів розслідування. Зокрема, виконання завдання «Профілактика протиправних дій» спрямоване на здійснення заходів щодо усунення причин та умов учинення шахрайства у сфері використання інтернет-банкінгу. Серед них слід виокремити:

1) виявлення осіб, схильних до антисуспільної поведінки в ІТ-сфері, та їх внесення у відповідні обліки Департаменту кіберполіції Національної поліції України;

2) запровадження дискусій у цифрових і друкованих засобах масової інформації стосовно питань впливу кіберзлочинності на соціум і суспільні відносини;

3) інформування громадян у соціальних мережах та месенджерах з приводу фактів учинення шахрайства у сфері використання інтернет-банкінгу (фішинг, спамінг).

Також з’ясовано, що тактичне завдання «Встановлення шахрая» спрямоване на проведення низки процесуальних дій і заходів. Серед них варто виокремити такі, як: огляд ЕОТ потерпілого (комп’ютера, смартфона, планшета); огляд і долучення до справи відеозаписів, фотографій; аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі); візуальне спостереження за особою; негласне зняття інформації з транспортних телекомунікаційних мереж тощо.

Крім того, акцентовано увагу на тому, що тактичне завдання «Встановлення співучасників в організованій групі чи злочинній організації» має важливе значення для встановлення ролі кожного з учасників у злочинному угрупованні. Адже завдяки з’ясуванню розподілу їх обов’язків можна вийти як на організаторів, так і на звичайних виконавців (шахраїв, спамерів), через яких здебільшого й буде отримано більшість доказової інформації.

Констатуючи вищенаведене, зазначимо, що початковий етап розслідування має досить важливе значення для кримінального провадження в цілому з огляду на те, що від ефективності реалізації усіх можливих дій (СРД, НСРД, інших процесуальних та пошукових заходів), які повинні бути проведені під час нього, залежить кількість та якість отримання доказової інформації. Вказано, що відомості про особу шахрая можливо отримати від потерпілого або свідків (очевидців) з приводу усіх можливих обставин вчиненого шахрайства у сфері використання інтернет-банкінгу. Зауважено, що на початковому етапі розслідування досліджуваного виду шахрайства необхідно реалізувати наступні заходи: допит потерпілого; огляд ЕОТ потерпілого (комп’ютеру, смартфону, планшету); огляд та долучення до справи відеозаписів, фотографій; розшук та встановлення особи шахрая; аудіо-контроль особи шляхом встановлення технічних засобів в публічно недоступному місці (транспортному засобі, квартирі); візуальне спостереження за особою; негласне знаття інформації з транспортних телекомунікаційних мереж; призначення експертиз.

3.2. Організаційно-тактичне забезпечення проведення процесуальних дій на подальшому етапі розслідування шахрайства у сфері використання інтернет-банкінгу

Подальший етап розслідування починається, як вказує переважна більшість вчених-криміналістів, з моменту пред'явлення особі підозри. В той же час, деякі науковці вказують інший момент початку реалізації вказаного етапу. Стосовно кримінальних проваджень за фактом вчинення шахрайства у сфері використання інтернет-банкінгу також є певні дискусійні аспекти, які стосуються зазначеного питання. Крім того, потрібно визначити перелік процесуальних дій та заходів, які необхідно провести на вказаному етапі, для забезпечення найбільш об'єктивного процесу розслідування [103, с. 145].

Стосовно подальшого етапу розслідування А. Ф. Волобуєв відмічав, що вказаний етап «…починається з моменту повідомлення особі про підозру у вчиненні злочину. До головних завдань подальшого етапу розслідування можуть бути віднесені такі: 1) формування системи доказів з обвинувачення особи в учиненні злочину (будуть відображені в обвинувальному акті); 2) установлення всіх співучасників злочину та збір доказів для їх обвинувачення; 3) забезпечення відшкодування заподіяних збитків, збір інформації про особистість підозрюваного (обвинуваченого). У кожній окремій методиці розслідування на цьому етапі розглядаються типові слідчі ситуації та комплекси слідчо-розшукових дій, що їм відповідають. Типові слідчі ситуації подальшого етапу розслідування визначаються позицією, яку займає особа, якій було повідомлено про підозру у вчиненні злочину» [63, с. 13].

В свою чергу, окрема група науковців (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) зауважує, «…завдання подальшого збирання, дослідження, оцінки і використання доказів, встановлення усіх елементів предмету доказування вирішується на наступному етапі. Тактика

слідчих (розшукових) дій може змінюватися залежно від зміни завдань, які стоять перед ними і обумовлюється слідчою ситуацією. Усе це знов-таки вимагає відмовитися від будь-якого шаблону в діяльності слідчого. Розслідування – процес творчий. У ньому немає місця схематизму, непродуманим аналогіям, наслідуванню та швидкоплинним рішенням. Окрема методика не повинна сковувати ініціативу слідчого. Вона завжди є лише комплексом рекомендацій, творча реалізація яких дозволяє уникнути помилок» [75, с. 201].

Зі свого боку, А. П. Шеремет відзначив, що «…характер типових слідчих ситуацій на наступному етапі розслідування в основному визначається результатами першочергових слідчих дій. В одних випадках основним напрямом розслідування є розшук уже встановленого злочинця, в інших – все ще невстановленого, в третіх – спрямованість на збирання додаткових фактичних даних. На даному етапі здійснюється планування розслідування за обраним напрямом, проводяться відповідні слідчі дії. Слідчий перебуває у тісному взаємозв’язку з органами дізнання та завершує збір і попередню оцінку доказів» [169, с. 337]. Досить цікавою в розрізі зазначеного вважаємо дімку колективу вчених-криміналістів під керівництвом В. Ю. Шепітька, які відмітили, що діяльність уповноваженої особи на подальшому етапі розслідування повинна розпочинатися з аналізу та «…оцінки зібраних фактичних даних, урахування нових слідчих ситуацій, визначення подальшого спрямування розслідування. Типовими слідчими ситуаціями на цьому етапі розслідування можуть бути такі: встановлено конкретну особу та її причетність до вчиненого шахрайства, пред’явлено обвинувачення; є підозрюваний, зібрані докази, але їх недостатньо для встановлення причетності підозрюваного до вчиненого шахрайства, обвинувачення не пред’явлено; зібрано недостатньо доказів, немає підозрюваного,не встановлено особу злочинця; зібрані докази свідчать про відсутність складу злочину (шахрайства) у діях підозрюваного. Якщо особа підозрюваного встановлена, то можуть мати місце такі типові слідчі ситуації

при розслідуванні шахрайства: підозрюваний визнає себе винним; підозрюваний не визнає себе винним» [62, с. 454].

Також варта уваги позиція В. В. Сисолятіна, який зазначив, що «…всі слідчі (розшукові) дії, негласні слідчі (розшукові) дії та інші процесуальні дії, а також розшукові заходи при розслідуванні кримінальних правопорушень, пов'язаних з використанням Інтернет-банкінгу, будемо розглядати відповідно до вказаного поділу. По досліджуваній категорії кримінальних проваджень є ряд беззаперечно важливих дій, які необхідно швидко та ефективно реалізовувати. Серед них необхідно виокремити допит підозрюваного для з'ясування механізму та обставин вчинення протиправного діяння, одночасний допит раніше допитаних осіб та обшук» [173, с. 89]. А вже С. І. Марко вказав, що наступний етап розслідування «…відповідно до загальних положень криміналістичної методики може мати два напрями розвитку: 1) якщо злочин не вдалося розслідувати по «гарячих слідах», типовими є такі слідчі (розшукові) дії та заходи: доручення оперативним підрозділам встановити особу злочинця, свідків, місце знаходження майна чи грошових коштів, отриманих злочинним шляхом; проведення повторних та додаткових слідчих (розшукових) дій, проведення негласних слідчих (розшукових) дій тощо; 2) якщо особу шахрая встановлено та затримано, типовими є такі слідчі (розшукові) дії та заходи: повідомлення про підозру та допит підозрюваного, обрання запобіжного заходу, вжиття інших необхідних заходів забезпечення кримінального провадження, обшук підозрюваного за місцем проживання, за місцем роботи з метою виявлення предметів злочину, слідів злочину, порівняльних зразків, пред'явлення підозрюваного для впізнання потерпілим і свідкам, одночасні допити, призначення ідентифікаційних, судово-психіатричних та інших видів судових експертиз, проведення слідчого експерименту тощо» [60, с. 748]. Як бачимо, більшість науковців, дослідження яких ми привели до розгляду, підтримують позицію, що подальший етап розслідування починається з моменту пред'явлення особі підозри.

Стосовно процесуальних дій та заходів, які необхідно проводити на подальшому етапі розслідування шахрайства у сфері використання інтернет-банкінгу нами було визначено наступні:

– допит підозрюваного;

– пред'явлення особи для впізнання (по фотознімкам, в натурі, за голосом);

– обшуки за місцем проживання чи перебування підозрюваного;

– огляд ЕОТ (комп'ютери, смартфони, планшети, жорсткі диски);

– тимчасовий доступ до речей та документів;

– одночасний допит раніше допитаних осіб;

– призначення та проведення судових експертиз.

Стосовно пред'явлення підозрюваного для впізнання варто привести твердження В. Ю. Шепітька, який вірно вказував, що «…шахраї досить часто змінюють свій зовнішній вигляд перед вчиненням злочину, одягають невластивий їм одяг; змінюють зачіску, відпускають бороду чи вуса, надягають окуляри. Тому при пред'явленні їх для впізнання впізнаючому необхідно дати можливість спокійно і уважно ознайомитися із зовнішністю осіб, яких йому пред'являють. Пред'являються для впізнання також окремі речі чи предмети, що могли належати потерпілому» [62, с. 455]. Відносно заходів підготовчого етапу пред'явлення для впізнання ми поділяємо позицію К. О. Чаплинського, який серед них виокремив наступні: «…попередній допит особи, яка впізнає (потерпілий, свідок); прийняття рішення про проведення впізнання; визначення місця, часу та способу проведення впізнання; визначення черговості пред'явлення для впізнання (якщо кілька злочинців); створення оптимальних умов для проведення даної слідчої дії; визначення способу фіксації ходу та результатів впізнання; підготовка необхідних науково-технічних засобів; забезпечення безпеки осіб, які приймають участь в даній слідчій дії; залучення (у необхідних випадках) спеціалістів або перекладача; підбір об'єктів (статистів), серед яких необхідно провести впізнання; складання плану проведення впізнання;

залучення понятих (не менше двох); проведення інструктивної наради (інструктаж) серед усіх учасників даної слідчої дії» [152, с. 10-11].

З приводу окремих елементів підготовчого етапу, В. В. Сисолятін вірно вказує, що «…основною особливістю пред'явлення для впізнання підозрюваного при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, обов'язкове його проведення буде у випадках можливості встановлення потерпілим тотожності правопорушника за голосом (у випадках телефонної розмови) або в натурі (у випадках розмови за допомогою відео-конференції)» [173, с. 89]. В той же час, опрацювання матеріалів судово-слідчої практики дозволило нам зробити висновок, що пред'явлення для впізнання в кримінальних провадженнях за фактом вчинення шахрайства у сфері використання інтернет-банкінгу у переважній більшості випадків (86 % від усіх пред'явлень) проводилось за фотознімками. З іншого боку, варто акцентувати увагу на обов'язковій реалізації пред'явлення підозрюваного для впізнання за фотографією та голосом.

Серед інших процесуальних дій, які потрібно проводити на подальшому етапі розслідування шахрайства, В. Ю. Шепітько виокремив допит підозрюваного. На час допиту, як вказував автор, уповноважена особа вже має необхідну інформацію про подію протиправного діяння, а також зібрано необхідні докази для викриття допитуваного у вчиненні шахрайства. Уповноважена особа, на думку дослідника, може використовувати ряд тактичних прийомів, як-от: постановку контрольних запитань, пред'явлення доказів (у тому числі різного роду документів), оголошення показань свідків» [62, с. 455]. В свою чергу, К. О. Чаплинський на основі опрацювання результатів анкетування працівників правоохоронних органів з'ясував, що серед найбільш розповсюджених тактичних прийомів допиту підозрюваного є такі як: «…встановлення психологічного контакту – 100% респондентів; викладання показань у формі вільної розповіді – 94%; постановку запитань – 100%; створення напруги – 47%; використання різних темпів допиту – 36%;

спостереження за поведінкою допитуваного та його психофізичними реакціями – 39%; пред'явлення доказів – 87%; використання фактора раптовості – 63%; актуалізацію забутого у пам'яті допитуваних – 57%; створення уявлення про інформованість слідчого – 28%; розповідь слідчим версій про учинений злочин або ймовірний розвиток події – 18%; приховування меж інформованості слідчого – 59%; використання конфліктів у злочинній групі – 21%; застосування науково-технічних засобів – 21%» [153, с. 164-165].

З огляду на зазначене вважаємо за потрібне навести безконфліктні та конфліктні ситуації допиту підозрюваного [Додаток А], а саме:

– підозрюваний добровільно надає інформацію про обставини шахрайських дій, конфліктна ситуація відсутня (21 %);

– підозрюваний викладає відомості про обставини вчинення шахрайських дій, але не пояснює її у повному об'ємі (7 %);

– підозрюваний не надає повні та правдиві покази (29 %);

– підозрюваний цілком відмовляється від комунікації з уповноваженою особою та від дачі свідчень (34 %);

– підозрюваний не спростовує факт і зміст шахрайських дій, але спростовує свою участь у їх скоєнні (9 %).

Для вирішення конфліктних ситуацій доцільно використовувати низку тактичних прийомів допиту. На основі опрацювання анкетування працівників правоохоронних органів [Додаток А] було підсумовано, що під час розслідування шахрайства у сфері використання інтернет-банкінгу ними використовуються наступні тактичні прийоми, зокрема:

– встановлення психологічного контакту – 96 %;

– застосування фактора раптовості – 61 %;

– створення уявлення про інформованість уповноваженої особи – 91 %;

– пред'явлення речових доказів та матеріалів справи – 29 %;

– зміна темпу допиту (зі швидкого на повільний та навпаки) – 47 %;

– створення напруги – 72 %;

– використання відеозапису – 38 %.

Відносно пред’явлення речових доказів та матеріалів справи, який ми вважаємо одним з найбільш ефективних тактичних прийомів для вирішення конфліктних ситуацій допиту підозрюваного, відмітимо, що серед них варто демонструвати такі об’єкти, як-от:

– протоколи допитів потерпілих і свідків;

– жорсткі диски та флеш-накопичувачі з відомостями про операції з інтернет-банкінгу;

– протоколи пред’явлення підозрюваного для впізнання з позитивним наслідком (особу впізнано за фото, голосом чи в натурі);

– скріншоти з хмарних сховищ;

– скріншоти переписки з потерпілими.

Для прикладу, на початку серпня 2020 року, перебуваючи за місцем свого проживання гр. Й. в мережі Інтернет, маючи необхідні знання в користуванні ЕОТ, а саме в роботі з персональним комп’ютером, в тому числі ноутбуком та мобільним телефоном, які підключені до світової мережі Інтернет, використовуючи логін та пароль для входу в соціальну мережу «Instagram», який використовується користувачами, в тому числі як електронний магазин по продажу різного роду товару, при цьому не маючи в наявності жодного товару, створюючи фейкові сторінки з подібними назвами реальних інтернет-магазинів, зв’язувалась з потерпілими, які бажали придбати товар. Зокрема, гр. Й. створила фейкові сторінки у соціальній мережі «Instagram», які мають облікові записи під різними назвами. Надалі, шахрайка видавала себе адміністратором або працівником вказаних інтернет-магазинів (згідно пролайканих постів на сторінках магазинів, залишених коментарів та кількістю підписників на сторінках інтернет-магазинів), ззовні копіювала сторінку інтернет-магазину, копіюючи у себе на фейкових сторінках всі запропоновані товари магазинів, тобто вела підготовку своїх фейкових сторінок до функціонування. Потерпілі зв’язувались з гр. Й. через соціальну мережу «Instagram» у вбудованому месенджері «Direct», де були

розміщені фейкові сторінки Інтернет магазинів, або через месенджери «Viber», «WhatsApp», де в ході спілкування з потерпілими засобами «Viber», «WhatsApp» та «Instagram», остання вводила учасників Інтернет покупок в оману, запевняючи потерпілих про правдивість викладеної нею інформації на сторінках фейкових. Шахрайка, повідомивши недостовірні дані відносно отримання останньою шкіряної жіночої сумки «Hermes» після оплати її вартості, та надала реквізити банківської картки, на яку необхідно здійснити перерахування грошових коштів у сумі 1000 грн. як оплату за придбане майно [143]. Після затримання гр. Й. в якості підозрюваної остання не бажала давати показання, але після пред'явлення скріншотів переписки з потерпілою, шахрайка почала надавати правдиві покази.

Крім того, було запропоновано перелік питань, які необхідно з'ясувати під час допиту підозрюваного, а саме:

1) які способи застосовувалися для входу в застосунок інтернет-банкінгу (використання спам-ботів; реквізитів картки, одержаної від конкретного потерпілого шляхом шахрайських дій; використання реквізитів картки, отриманої з web-сторінок підставних інтернет-магазинів);

2) у який спосіб вчинено шахрайські дії (шляхом отримання доступу до ЕОТ з паролями, які встановив потерпілий; шляхом використання мережі Wi-Fi);

3) чи вчинено шахрайські дії організованою групою або злочинною організацією; якщо так, то яка структура злочинного угруповання;

4) який статус та обов'язки кожного зі співучасників шахрайства;

5) яким чином розподілялися викрадені майно та грошові кошти між співучасниками;

6) протягом якого проміжку часу було вчинено шахрайські дії;

7) наявність учинення супутніх кримінальних правопорушень;

8) які знаряддя й засоби використовувались під час учинення шахрайських дій (комп'ютери, смартфони, модеми, маршрутизатори, браузери, спам-боти);

9) яка загальна сума грошових коштів була отримана шляхом реалізації шахрайських дій у сфері використання інтернет-банкінгу тощо.

Крім того, було охарактеризовано організаційно-тактичне забезпечення проведення одночасного допиту двох або більше раніше допитаних осіб, а саме встановлено, що вказана процесуальна дія повинна бути спрямована на усунення невідповідностей у показаннях раніше допитаних осіб [Додаток А], зокрема:

1) підозрюваного та потерпілого (87 %) – як було вчинено шахрайські дії; які було застосовано засоби для їх учинення (комп'ютер, планшет, ноутбук, смартфон) тощо;

2) між підозрюваними (9 %) – які ролі в організованій групі чи злочинній організації вони виконували тощо;

3) підозрюваного та свідка (2 %);

4) потерпілого та свідка (1 %);

5) між потерпілими (1 %).

Також було з'ясовано, що тимчасовий доступ до речей і документів уможливлює подальше призначення та проведення експертизи, що дозволить виконати низку завдань кримінального провадження, а саме:

1) встановити всі використані ЕОТ під час учинення шахрайських дій у сфері використання інтернет-банкінгу;

2) дослідити платіжні перекази для виявлення латентних платежів;

3) дослідити програмне забезпечення ЕОТ;

4) отримати доступ до особистих і банківських облікових записів у комп'ютерній системі (акаунтів), що були створені для проведення інтернет-банкінгу.

Відносно проведення обшуку в кримінальних провадженнях досліджуваної категорії ми повністю поділяємо позицію Т. В. Коршикової, яка зауважила, що «…виходячи зі способів вчинення шахрайств, під час яких використовується ЕОТ, варто мати на увазі, що відправлення та передача інформації про предмет шахрайства, а також в окремих випадках спілкування

між потерпілим і злочинцем, здійснюються в електронній формі, зокрема за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем. Саме тому, для виявлення ЕОТ, з якої було здійснено відправлення та передачу інформації, засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, що використовувались з метою вчинення таких видів шахрайств, важливе місце належить обшуку, що сприяє виявленню доказової та орієнтуючої інформації. Обшук у кримінальних провадженнях про шахрайство, що вчиняється з використанням ЕОТ, має свою специфіку, що визначається самим видом кримінального правопорушення, так як місця обшуку можуть бути різними. Як правило, обшуки у кримінальних провадженнях за фактом шахрайства, учиненого з використанням ЕОТ, здійснюються: за місцем проживання підозрюваного; у місцях, які використовувались підозрюваним для виходу у мережу Інтернет під час вчинення шахрайства; місцях зберігання ЕОТ, яка була використана з метою вчинення шахрайства; осіб, які були причетні до створення та подальшого адміністрування сайтів, які використовувались у подальшому з метою вчинення шахрайства» [49, с. 521].

В розрізі зазначеного вважаємо за необхідне навести перелік місць, де варто проводити обшук [Додаток Б], а саме:

– місця зберігання та обробки даних про використання інтернет-банкінгу (сервери відповідних банківських установ, ЕОТ шахраїв) – 65 %;

– місця знаходження ЕОТ, яку використовували для вчинення шахрайських дій, – 43 %;

– місця зберігання відомостей, отриманих злочинним шляхом, – 38 %.

Для прикладу, гр. Г. приблизно впродовж квітня 2020 року, маючи навички роботи із комп’ютерною технікою та інтернет-ресурсами, з використанням ЕОТ (мобільного телефону «Samsung») та підключення до мережі Інтернет, знаходячись в державній установі «Запорізькій слідчій ізолятор», зареєструвався в Інтернет мережі на сайті оголошень «OLX», який діє на території України, та розмістив оголошення та отримав логін і пароль

для входу на зареєстровану сторінку на сайті оголошень «OLX», з метою подальшого незаконного заволодіння коштами потенційних клієнтів шляхом їх обману, розмістив на вказаному сайті завідомо неправдиву інформацію у вигляді оголошення щодо продажу різноманітних, які насправді не мав в наявності та не мав мети подальшої їх реалізації, шляхом продажу. Так, 09.04.2020 року, потерпілий гр. Ю., перебуваючи на сайті оголошень «OLX», знайшов оголошення про продаж скутера, яке було розміщено на сайті оголошень шахраєм за загальною ціною від 6000 до 38000 грн. В той же день, будучи введеним в оману, потерпілий в ході розмови по телефону з шахраєм, виявив бажання та домовився про купівлю вказаного скутера, при цьому умовою угоди була пересилка товару за допомогою перевізника «Нова Пошта», протягом декілька днів з доставкою до дому з моменту замовлення та оплата за бронювання скутера. В свою чергу, повідомив потерпілому, що він повинен попередньо оплатити бронювання товару, а саме грошові кошти в сумі 1000 грн. на банківську картку емітовану АТ КБ «Приватбанк», оформлену на ім’я гр. Д., яка, в свою чергу використовувалася шахраєм шляхом встановленого застосунку до інтернет-банкінгу «Приват 24» [140]. Під час проведення обшуку у гр. Г. було виявлено вказаний телефон з усіма наявними відомостями.

Підводячи підсумок, зазначимо, що подальший етап розслідування шахрайства у сфері використання інтернет-банкінгу починається з моменту пред’явлення особі підозри.

Стосовно процесуальних дій та заходів, які необхідно проводити на подальшому етапі його розслідування, було визначено наступні: допит підозрюваного; пред’явлення особи для впізнання (по фотознімкам, в натурі, за голосом); обшуки за місцем проживання чи перебування підозрюваного; огляд ЕОТ (комп’ютери, смартфони, планшети, жорсткі диски); тимчасовий доступ до речей та документів; одночасний допит раніше допитаних осіб; призначення та проведення судових експертиз.

3.3. Особливості використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу

Ефективна реалізація кримінальних проваджень будь-якої категорії іноді напряму залежить від раціонального використання спеціальних знань. Під час розслідування шахрайства у сфері використання інтернет-банкінгу дослідження вказаної наукової категорії є обов'язковим, оскільки впливає на оптимальний збір доказової інформації як на початковому, так і на подальшому етапі кримінального провадження [102, с. 121].

Як вірно вказує С. В. Чучко, «…процес розслідування кримінальних правопорушень може характеризуватися проведенням різноманітних процесуальних дій. Деякі з них направлені на вилучення та перевірку певної доказової інформації. Під час їх проведення в уповноважених осіб (слідчого, дізнавача, прокурора) може виникнути потреба у з'ясуванні окремих обставин, які викликають необхідність у наявності спеціальних знань. Так, вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет в Україні характеризується багатьма аспектами, які вимагають володіння вказаними знаннями. Іноді без них взагалі неможливо довести вину шахрая. Адже специфічні спосіб та умови вчинення кримінального правопорушення (мережа Інтернет), характерна слідова картина для такої категорії проваджень (ідеальні та віртуальні докази) зумовлюють необхідність залучення фахівців з різних галузей науки для максимально ефективного вилучення доказової інформації» [163, с. 234].

Спираючись на вищенаведене, вважаємо обґрунтованою позицію Г. С. Бідняк, яка наголошувала, що «…поняття спеціальних знань не закріплено в жодному нормативно-правовому акті та вирізняє наступні їх ознаки: 1) є комплексом знань і навичок у різних галузях; 2) складаються з системи відомостей в галузі науки, техніки та інших сфер людської діяльності; 3) використовуються в досудовому розслідуванні та судовому

провадженні у випадках і в порядку, визначених кримінальним процесуальним законодавством; 4) їх використання здійснюється у взаємозв'язку з науково-технічними засобами; 5) реалізуються визначеним суб'єктом кримінального судочинства у процесі практичної діяльності, спеціальної підготовки з урахуванням професійного досвіду і засновані на системі теоретичних знань у відповідній галузі; 6) їх реалізація вимагає значних витрат часу й інтелектуальних зусиль; 7) сприяють у розробці технічних засобів і прийомів роботи з доказами та встановленню вагомих обставин, що мають значення для доказування» [5, с. 41–44].

А вже Д. В. Пашнєва вказує на те, що «…форми використання спеціальних знань можуть бути диференційовані на обов'язкове і факультативне залучення їх під час проведення процесуальних дій. Окрім того, як зазначає автор, процесуальні форми використання спеціальних знань поділяються за характером дій, при проведенні яких вони застосовуються, на ті, що використовуються при проведенні слідчих та інших процесуальних дій. Непроцесуальні форми застосування спеціальних знань можуть бути розділені за ознаками сфери використання і суб'єкта їх застосування» [95, с. 89]. Тобто науковець розділяє форми використання спеціальних знань на окремі категорії: процесуальні та не процесуальні.

Зокрема, І. І. Когутич серед головних процесуальних форм використання спеціальних знань вирізняє наступні: «1) безпосереднє використання їх слідчим, прокурором, складом суду під час виконання своїх процесуальних функцій збирання, дослідження та оцінки доказів; 2) участь спеціаліста у провадженні СРД; 3) призначення і провадження судових експертиз. Серед непроцесуальних форм доцільно розглядати: 1) консультативну та довідкову діяльність суб'єктів спеціальних знань; 2) проведення ревізій чи аудиторських дій; 3) участь суб'єктів спеціальних знань в ОРЗ; 4) попередні дослідження матеріальних об'єктів спеціалістами та експертами; 5) результати перевірок за криміналістичними обліками» [46, с. 113–114].

Зі свого боку, Л. Ш. Мамедова акцентувала увагу на тому, що під час розслідування кіберзлочинів «…необхідно більше уваги приділити дослідженню так званої цифрової криміналістики (digital forensics), оскільки знання специфіки роботи цифрових криміналістичних засобів і вміння використовувати всі їхні властивості є найважливішою умовою якісного вирішення криміналістичних завдань, що стоять перед спеціалістом, фахівцем (експертом) під час розслідування кіберзлочинів. Крім того, з метою ефективного розслідування та розкриття зазначеної категорії злочинів доцільно приділити увагу підвищенню кваліфікації експертів і спеціалістів, створити передумови для впровадження єдиної системи підготовки та підвищення кваліфікації кадрів, які залучаються до протидії кіберзлочинності. Важливо, ураховуючи специфіку проведення судової експертизи, зокрема цифрових криміналістичних експертиз, створити умови для їхнього розвитку та розробити єдині методи проведення судових експертиз під час розслідування зазначеної категорії злочинів шляхом удосконалення науково-методичних рекомендацій відповідно до міжнародних стандартів. Для вирішення цих питань потребує ретельного дослідження визначення таких понять, як «спеціаліст», «фахівець» та «експерт», а надалі – досягнення узгодженості їхнього правового статусу у чинному законодавстві зарубіжних країн та України» [79, с. 394].

Досить цікавою є позиція К. О. Чаплинського, Н. В. Павлової та Д. А. Птушкіна, які зауважують, що «…шахраї нерідко використовують комп’ютерну техніку 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 тощо. На флеш-карті мобільного телефону також може зберігатися значна кількість інформації про контакти, зв’язки. Визначена інформація, безсумнівно, становить інтерес для правоохоронних органів та спрямовує їх діяльність у вірному напрямку» [94, с. 135].

Підводячи підсумок, зазначимо, що використання спеціальних знань має досить важливе значення під час розслідування шахрайства у сфері використання інтернет-банкінгу. Серед форм його використання розрізняють процесуальні та організаційні.

Найбільш оптимальною вважаємо думку С. С. Чернявського, який виділив та здійснив аналіз наступних форм використання спеціальних знань у справах про фінансове шахрайство, зокрема: «…участь спеціалістів при проведенні попередньої перевірки інформації про злочин; консультації фахівців при підготовці та проведенні слідчих дій; призначення і проведення документальних ревізій та інших перевірок; призначення судових експертиз. У 91,0 % справ допомога спеціаліста використовувалась у різних формах: фахівці залучалися до проведення слідчих дій (14,2 %); давали поради та консультації (78,8 %); були допитані стосовно обставин, пов'язаних з їх професійною діяльністю (17,3 %)» [158, с. 19].

Через призму вищенаведених позицій вчених-криміналістів серед основних форм використання спеціальних знань у кримінальному провадженні нами виокремлено такі:

а) безпосереднє застосування уповноваженою особою спеціальних знань під час реалізації окремих слідчих (розшукових) дій, НСРД та інших процесуальних і розшукових заходів;

б) залучення спеціаліста до проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій і розшукових заходів;

в) консультативна допомога спеціаліста;

г) призначення та проведення судових експертиз.

В свою чергу, Т. В. Коршикова акцентує увагу на тому, що «…у місцях, де вчиняються такі види шахрайств, є ЕОТ, тому потреба в допомозі спеціаліста-консультанта якими, як правило, виступають експерти комп'ютерно-технічного відділу Експертної служби МВС України, виникає на початковому етапі досудового розслідування, коли слідчому необхідно оглянути ЕОТ, насамперед, яка знаходиться в робочому (увімкненому) стані.

У цьому випадку спеціаліст повинен надати допомогу: в огляді ЕОМ на стадії її виявлення, у т.ч. встановити в ЕОТ наявність зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність модему тощо); фіксування усіх дій з ЕОТ за допомогою фото- та відеотехніки; здійснення опису екрану та прилеглої обстановки; копіювання наявної в ЕОТ інформації; вжиття заходів щодо встановлення пароля доступу до захищених програм; належного та безпечного вимикання ЕОТ; вилучення, упакування та опечатування ЕОТ, інших носіїв інформації (накопичувачі на жорстких і гнучких магнітних дисках, компакт-диски, DVD-диски, ZIP-дискети тощо) та інших предметів і документів для їх дослідження в лабораторних умовах; способів транспортування (перевезення) вилучених предметів» [55, с. 297].

Опрацювання матеріалів судово-слідчої практики [Додаток Б] дало змогу зробити висновок, що спеціаліста залучали до проведення таких дій:

– огляд місця події – 100 %;

– огляд ЕОТ – 100 %;

– тимчасовий доступ до речей і документів – 62 %;

– обшук – 65 %;

– допит – 14 %;

– одночасний допит раніше допитаних осіб – 9 %;

– аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці – 100 %;

– зняття інформації з транспортних телекомунікаційних мереж та електронних систем – 100 %.

З огляду на вказане, ми вважаємо за потрібне внести зміни до ч. 1 ст. 71 КПК України для процесуального закріплення статусу спеціаліста, який би відповідав сучасним викликам і реаліям, особливо в кримінальних провадженнях щодо шахрайства у сфері використання інтернет-банкінгу. Тому пропонуємо викласти ч. 1 ст. 71 КПК України в такій редакції: «Спеціалістом у кримінальному провадженні є особа, яка володіє

спеціальними знаннями та навичками, що можуть бути застосовані під час досудового розслідування та судового розгляду шляхом надання довідок, пояснень, консультацій і висновків в усній чи письмовій формі для вирішення питань, що вимагають володіння відповідними спеціальними знаннями чи навичками».

Для прикладу, гр. Є. шляхом незаконних операцій з використанням ЕОТ створив в месенджері «Telegram»-канал, де свідомо опубліковував неправдиві дописи про можливість інвестування грошових коштів із подальшим прибутком їх через певний час, хоча такі можливості у нього були відсутні, зазначивши як засіб зв’язку із ним для отримання послуги, акаунт в месенджері «Telegram». З метою здійснення протиправної діяльності шахраєм було придбано необхідну комп’ютерну техніку, а саме: мобільний телефон марки «IPhone», з якого здійснювався зв'язок із потерпілими, а також здійснювався вихід до мережі Інтернет на спеціально створений телеграм-канал в месенджері «Telegram», де опубліковувались неправдиві дописи про можливість інвестування грошових коштів із подальшим прибутком їх через певний час. Придбана ЕОТ забезпечувала йому розміщення дописів про інвестицію коштів та зв’язок із потерпілою гр. Д., у ході спілкування з якою шахрай запевняв останню в правдивості виплати, попередньо домовившись про необхідність отримання банківських карток сторонніх осіб, із подальшим їх використанням в інтернет-банкінгу, для здійснення перерахунку на такі грошових коштів отриманих від потерпілої, з подальшим перерахуванням коштів на інші картки, з метою маскування своєї незаконної діяльності [138]. Під час розслідування вказаного факту шахрайських дій спеціаліст в галузі комп’ютерних технологій вилучив у шахрая мобільний телефон, комп’ютер (системний блок у зборі із комплектуючими) та ноутбук марки «Макбук Про».

Окрема група вчених науковців (Є. І. Макаренко, О. В. Негодченко, В. М. Тертишник) зауважила, що вірний підбір часу «…передбачає врахування таких обставин: своєчасність призначення експертизи;

властивості та стан об’єктів експертного дослідження; необхідність і можливість отримання порівняльних зразків; особливості експертного дослідження (складність, наявність відповідних методик, час проведення та ін.); слідча ситуація; наявність або відсутність необхідних матеріалів для призначення експертизи» [76, с. 37].

Зі свого боку, К. І. Говорова вказала на те, що «…використання комп’ютерних технологій у сфері платежів є характерною ознакою сучасного життя. Банківські послуги, які надають клієнтові дистанційно, а також платежі, що здійснюють без участі готівки, прискорюють обіговість, скорочують кількість грошових коштів, необхідних в обігу. Це, як результат, знижує витрати обігу, збільшує прозорість розрахунків. Завдяки своїй простоті, масовості, доступності технологій, подібні банківські операції все більше приваблюють шахраїв. У зв’язку із цим суттєво зростає кількість злочинів у банківській сфері з використанням Інтернету. У сучасній юридичній літературі для відокремлення цієї категорії злочинів найчастіше вживають термін «кіберзлочинність у банківській сфері». Аналізуючи зарубіжний досвід боротьби з кіберзлочинністю, стає чітко видно, що вона (кіберзлочинність) має тенденцію до зростання. Однією з причин її зростання є постійне вдосконалення технічних систем глобального зв’язку та прямий доступу користувачів до комп’ютерних технологій через персональні комп’ютери» [12, с. 465].

В розрізі зазначеного наведемо тезу Ю. Ю. Нізовцева та О. С. Омельяна, які вказали, що «…кожна кібератака має свої особливості. Найбільш типові такі. Носії інформації атакованої системи (їх клони чи бітові образи) можуть бути основними носіями слідів кібератаки. Їх інформаційний вміст становлять, зокрема: шкідливі програмні засоби, їх залишки та/або сліди функціонування; нові файли, які з’явилися на носії під час кібератаки (поміщені на носій зловмисником); сліди чи залишки знищених під час кібератаки файлів; зашифровані під час кібератаки файли; логфайли, налаштування тощо. Зазвичай найбільших результатів досягають, коли

вилучають бітові образи носіїв інформації. Якщо ці носії відносно невеликого обсягу, на один носій криміналістичної інформації може бути поміщено кілька бітових образів. Переваги методу – оригінальні носії інформації не вилучаються, а автоматизована система, відновившись після кібератаки, може функціонувати далі. Недоліки – створення образів потребує багато часу» [90, с. 62].

Стосовно призначення експертиз в досліджуваній категорії кримінальних проваджень варто привести твердження Т. В. Коршикової, яка на основі вивчення результатів кримінальних проваджень щодо шахрайств, які вчиняються з використанням ЕОТ, визначила «…наступні види експертизи, які призначались при їх розслідуванні, зокрема щодо вилучених: електронно-обчислювальна техніка (комп'ютерно-технічна експертиза (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення), дактилоскопічна експертиза вилучених слідів рук з різних предметів ЕОТ); телекомунікаційні засоби та системи (експертиза телекомунікаційних систем і засобів); документи (експертиза документів, які утворювались внаслідок вчинення шахрайських дій – криміналістична почеркознавча експертиза; технічна експертиза документів; дактилоскопічна експертиза вилучених слідів рук з документів); майно, яке було предметом посягання (криміналістична експертиза матеріалів, речовин і виробів; трасологічна експертиза; дактилоскопічна експертиза вилучених слідів рук з різних предметів)» [53, с. 290].

Також ми підтримуємо позицію Ю. М. Чорноус, яка зауважила, що «…реалізація техніко-криміналістичного забезпечення стосується різних питань, пов'язаних із залученням спеціальних знань, участю спеціалістів (зокрема, інспекторів-криміналістів, судових експертів) при проведенні слідчих (розшукових) дій, вилученням речових доказів, наступним проведенням судових експертиз. Судово-експертна діяльність є предметом дослідження за змістом багатьох наукових робіт, заслуговує особливої уваги у структурі техніко-криміналістичного забезпечення, а згідно з іншою

точкою зору – як самостійна складова криміналістичного забезпечення. Таким чином, основний зміст техніко-криміналістичного забезпечення розслідування злочинів складають відповідні спеціальні знання та технічні засоби, а також суспільні відносини, що складаються у процесі їх застосування. Розвиток суспільних відносин, вплив науково-технічного прогресу, удосконалення засобів і методів злочинної діяльності вимагають постійної уваги до вказаних питань» [161, с. 221].

Відповідно до Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, «…до основних завдань експертизи комп'ютерної техніки і програмних продуктів під час досудового розслідування шахрайств, що вчиняються з використанням ЕОТ, належать: – установлення робочого стану комп'ютерно-технічних засобів; – установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; – виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; – установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку» [108].

Досить вірно Г. М. Яровенко та М. М. Бояджян вказали на те, що «…сьогодні питання протидії кібершахрайству в банківській сфері є актуальним і в Україні. На основі проведеного аналізу наслідків кібершахрайств, які відбуваються у сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії стає об'єктом шахрайства. Для боротьби із цим способом шахрайства українські банки не мають доволі дієвих інструментів. Як наслідок — призначення економічних експертиз документів фінансово-кредитних операцій, які проходять саме через інтернет-банкінг, і розширення змісту експертних завдань» [171, с. 836].

В свою чергу, А. В. Реуцький запропонував такий перелік об'єктів, які підлягають експертному дослідженню: «…документи – сліпи, платіжні

картки, гроші, цінні папери тощо; комп'ютерна техніка, у тому числі банкомати, POS-термінали, енкодери, автоматизовані торговельні термінали, ноутбуки, комунікатори, електронні записні книжки й перекладачі; різні типи друкувальних пристроїв – принтери, термопринтери, ембосери, імпринтери; різноманітні машинні носії інформації – дискети, диски, магнітні стрічки (мікрочипи) платіжних карток тощо; комп'ютерна інформація – програми, файли та ін.; речові докази – цифрові засоби електрозв'язку, пристрої радіозв'язку, сліди та їх копії, зразки, приєднані до кримінальної справи та ін.» [122, с. 14].

Окрема група дослідників (О. М. Стрільців, В. В. Крижна, О. В. Максименко) зазначила, що «…до об'єктів, які направляються на комп'ютерно-технічну експертизу у кримінальних провадженнях за фактом вчинення шахрайства з використанням ЕОТ, встановлено такі вимоги: – для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях; – системний блок комп'ютера та інші пристрої мають бути упаковані й опечатані в такий спосіб, що унеможливлює їхнє пошкодження, безпосередній доступ до носіїв інформації та підключення системного блока до мережі електроживлення; – у постанові про призначення експертизи повинні бути точно вказані місце, час вилучення, а також зовнішній вигляд пристроїв і програмних продуктів, які направляються на експертизу; – при вилученні комп'ютерів та електронних носіїв інформації їх варто упаковувати в поліетиленовий (або полотняний) пакет, який опечатують. Носії інформації можна упакувати в картонну чи пластмасову коробку та опечатати її. Варто зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їхня кількість). Коробку з носіями та опис поміщають до поліетиленового пакету, який заклеюють; – під час перевезення комп'ютерних засобів вживають заходів щодо запобігання їх механічного пошкодження і взаємодії з хімічно активними речовинами» [92, с. 56–57].

Інша група науковців (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков,

С. Ю. Петряєв) вказала, що «…у провадженнях даного виду в більшості випадків призначають криміналістичні (трасологічну, почеркознавчу), судово-бухгалтерську, судову експертизу комп'ютерної техніки і програмних продуктів і деякі інші види експертиз, техніко-криміналістичне дослідження документів. Традиційні трасологічні експертизи призначають з метою ідентифікації особи за слідами, вилученими з місця події, визначення механізму доступу до комп'ютерної техніки, дій правопорушника на об'єкті. З приводу криміналістичного дослідження документів науковці зазначили, що його призначають для дослідження ліцензійних угод, журналів реєстрації користувачів, апаратних журналів, роздруківок, записів і інших матеріалів на папері. Судово-бухгалтерські експертизи призначають для визначення розмірів завданого збитку, а експертиза комп'ютерної техніки і програмних продуктів проводиться з метою дослідження апаратного забезпечення системи ЕОМ, машинних носіїв, програм для ЕОМ і баз даних» [75, с. 483].

А вже С. В. Головкін обґрунтовував «…положення про доцільність використання комп'ютерних засобів у цифровій фотографії для фіксації, дослідження папілярних візерунків, а також виготовлення додатку до висновку дактилоскопічної експертизи. Визначені цілі та задачі, а також основні вимоги, що пред'являються до судової фотографії з урахуванням досягнень технічного прогресу. У зв'язку з широким впровадженням у криміналістику цифрової фотографії, обґрунтовується доцільність дослідження папілярних візерунків за допомогою комп'ютерного обладнання та його програмного забезпечення. У теперішній час застосування в ОВС цих технічних засобів, здійснюється на основі особистої ініціативи експертів без урахування наукових рекомендацій та узагальнення існуючої експертної практики» [13, с. 8].

З іншого боку, група вчених-криміналістів (О. В. Одерій, С. В. Самойлов) доречно зауважили, що «…через специфічність і різноплановість способів вчинення шахрайств із використанням мережі «Інтернет», необхідно орієнтуватись на призначення конкретних судових

експертиз і визначати коло питань, які можуть бути поставлені перед експертами» [130, с. 109]. В розрізі зазначеного, вважаємо досить вірною тезу С. В. Головкіна, який відмітив, що «…значення криміналістичних експертиз обумовлене багатьма чинниками, зокрема, призначення їх представляє собою ефективний напрям вирішення складних задач розслідування, за допомогою їх отримується інформація, яка може свідчити про причетність особи до події злочину, спонукати підозрюваного до дачі правдивих показань» [14, с. 115].

З приводу КТЕ вважаємо найбільш точною позицію О. А. Самойленко, яка відмічає, що вказана експертиза «…це дослідження технічних властивостей комп'ютерного (цифрового) обладнання, програмного забезпечення, інформації, що містяться на цифрових носіях, з метою встановлення фактичних даних, які мають значення для провадження та пов'язані із застосуванням комп'ютерної техніки, а також виявляються на підставі спеціальних знань у галузях комп'ютерної техніки та програмування. Об'єктами судової експертизи є комп'ютери з носіями інформації (будь-які накопичувачі інформації – дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (наприклад, мобільні телефони, банкомати, гральні автомати, карт-ридери, електронні записні книжки, пейджери, принтери тощо), а також документація до обладнання» [125, с. 159].

В свою чергу, О. І. Коваленко засвідчує, що «…існують такі розповсюджені способи підміни реальної IP-адреси: підключення до проксі-серверу, використання інтернет-браузера TOR, маскування IP-адреси через VPN. Під час КТЕ надзвичайно важливо виявити програмне забезпечення, що було встановлене для приховування IP-адреси. Прикладами вищевказаного можуть бути: ProxyCap, Proxyfier, Proxy Switcher - програми для проксі; TOR Browser, Tor Control (anonymity layer) for Firefox; NordVPN, OpenVPN, ExpressVPN, PureVPN for Teams, ProtonVPN, NetMotion – програми, які забезпечують сервіс VPN. Якщо експертом буде проведено якісне дослідження мережевих слідів та викрито усі ланцюжки IP-адрес,

через які проходили транзакції, з великою вірогідністю таке кримінальне правопорушення буде розкрито» [41, с. 265].

На підставі узагальнення матеріалів кримінальних проваджень [Додаток Б] запропоновано обов'язкові судові експертизи, що необхідно призначати під час розслідування шахрайства у сфері використання інтернет-банкінгу, а саме:

а) судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів, експертиза цифрової інформації, програмно-комп'ютерна експертиза);

б) судово-бухгалтерська експертиза;

в) інформаційно-комп'ютерна експертиза;

г) експертиза телекомунікаційних систем і засобів.

Висновки до розділу 3

Після дослідження організації і тактики проведення процесуальних дій під час розслідування шахрайства у сфері використання інтернет-банкінгу, варто зробити наступні висновки:

1. Розглянуто специфіку початкового етапу досудового розслідування, визначено особливості реалізації слідчих (розшукових) і процесуальних дій і розшукових заходів. Зауважено, що на початковому етапі розслідування шахрайства необхідно реалізувати низку заходів, серед яких варто виокремити такі, як допит потерпілого, огляд ЕОТ потерпілого, аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці тощо.

2. Розкрито особливості тактики огляду. Визначено основні ділянки, на яких можуть бути виявлені сліди шахрайських дій. Акцентовано увагу на тактиці огляду електронних відомостей, які перебувають або у відкритому доступі в мережі Інтернет, або на матеріальних носіях інформації чи

різноманітних серверах для їх зберігання. Зауважено, що під час огляду ЕОТ (ноутбук, смартфон, комп'ютер) об'єктом огляду може бути безпосередньо ЕОТ, так і відповідні носії інформації. Обґрунтовано тактичні завдання, що необхідно реалізовувати в кримінальному провадженні. Зокрема, виконання завдання «Профілактика протиправних дій» спрямоване на здійснення заходів щодо усунення причин та умов учинення шахрайства у сфері використання інтернет-банкінгу. Серед них слід виокремити: 1) виявлення осіб, схильних до антисуспільної поведінки в ІТ-сфері, та їх внесення у відповідні обліки Департаменту кіберполіції Національної поліції України; 2) запровадження дискусій у цифрових і друкованих засобах масової інформації стосовно питань впливу кіберзлочинності на соціум і суспільні відносини; 3) інформування громадян у соціальних мережах та месенджерах з приводу фактів учинення шахрайства у сфері використання інтернет-банкінгу (фішинг, спамінг).

3. З'ясовано, що тактичне завдання «Встановлення шахрая» спрямоване на проведення низки процесуальних дій і заходів. Серед них варто виокремити такі, як: огляд ЕОТ потерпілого (комп'ютера, смартфона, планшета); огляд і долучення до справи відеозаписів, фотографій; аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі); візуальне спостереження за особою; негласне зняття інформації з транспортних телекомунікаційних мереж тощо. Акцентовано увагу на тому, що тактичне завдання «Встановлення співучасників в організованій групі чи злочинній організації» має важливе значення для встановлення ролі кожного з учасників у злочинному угрупованні. Адже завдяки з'ясуванню розподілу їх обов'язків можна вийти як на організаторів, так і на звичайних виконавців (шахраїв, спамерів), через яких здебільшого й буде отримано більшість доказової інформації.

4. Розглянуто особливості здійснення комплексу СРД, НСРД, процесуальних і розшукових заходів та інших дій, спрямованих на

реалізацію завдань подальшого етапу розслідування. Наголошено, що подальший етап розслідування починається з моменту пред'явлення особі підозри. Виокремлено процесуальні дії та заходи, що необхідно проводити на подальшому етапі розслідування шахрайства у сфері використання інтернет-банкінгу, а саме: допит підозрюваного; пред'явлення особи для впізнання (за фотознімками, голосом, у натурі); обшук за місцем проживання чи перебування підозрюваного; огляд ЕОТ (комп'ютери, смартфони, планшети, жорсткі диски); тимчасовий доступ до речей і документів; одночасний допит раніше допитаних осіб; призначення та проведення судових експертиз.

5. Визначено найбільш ефективні тактичні прийоми допиту підозрюваного, зокрема: встановлення психологічного контакту – 96 %, застосування фактору раптовості – 61 %, створення уявлення про поінформованість уповноваженої особи – 91 %, пред'явлення речових доказів і матеріалів провадження – 29 %, зміна темпу допиту (із швидкого на повільний і навпаки) – 47 %, створення напруги – 72 %, використання відеозапису – 38 %. Наголошено на їх обов'язковому застосуванні для вирішення конфліктних ситуацій. Запропоновано перелік питань, які необхідно з'ясувати під час проведення допиту підозрюваного. Схарактеризовано організаційно-тактичне забезпечення проведення одночасного допиту двох або більше раніше допитаних осіб.

6. Доведено, що під час пред'явлення речових доказів і матеріалів провадження варто серед них демонструвати такі об'єкти: протоколи допиту потерпілих і свідків; жорсткі диски та флеш-накопичувачі з відомостями про операції з інтернет-банкінгу; протоколи пред'явлення підозрюваного для впізнання (особу впізнано за фотографією, голосом чи в натурі); скріншоти із хмарних сховищ; скріншоти переписки з потерпілими тощо. З'ясовано, що тимчасовий доступ до речей і документів уможливлює подальше призначення та проведення експертизи, що дозволить виконати низку завдань кримінального провадження, а саме: 1) встановити всі використані

ЕОТ під час учинення шахрайських дій у сфері використання інтернет-банкінгу; 2) дослідити платіжні перекази для виявлення латентних платежів; 3) дослідити програмне забезпечення ЕОТ; 4) отримати доступ до особистих і банківських облікових записів у комп'ютерній системі (акаунтів), що були створені для проведення інтернет-банкінгу. Наведено перелік місць, де варто проводити обшук, а саме: місця зберігання та обробки даних про використання інтернет-банкінгу (сервери відповідних банківських установ, ЕОТ шахраїв) – 65 %; місця знаходження ЕОТ, яку використовували для вчинення шахрайських дій, – 43 %; місця зберігання відомостей, отриманих злочинним шляхом, – 38 %.

7. Опрацьовано сутність і форми застосування спеціальних знань, а також з'ясовано участь спеціаліста під час проведення СРД, НСРД та інших процесуальних заходів. З-поміж основних форм використання спеціальних знань під час розслідування шахрайства виокремлено такі: а) безпосереднє застосування уповноваженою особою спеціальних знань під час реалізації окремих СРД, НСРД та інших процесуальних дій і розшукових заходів; б) залучення спеціаліста до проведення окремих СРД, НСРД та інших процесуальних дій і розшукових заходів; в) консультативна допомога спеціаліста; г) призначення та проведення судових експертиз.

8. Встановлено, що спеціаліста залучали до проведення таких дій: огляд місця події – 100 %, огляд ЕОТ – 100 %, тимчасовий доступ до речей і документів – 62 %, обшук – 65 %, допит – 14 %, одночасний допит раніше допитаних осіб – 9 %, аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці – 100 %, зняття інформації з транспортних телекомунікаційних мереж та електронних систем – 100 %. Підтримано позицію щодо внесення змін до ч. 1 ст. 71 КПК України для процесуального закріплення статусу спеціаліста, який би відповідав сучасним викликам і реаліям, особливо в кримінальних провадженнях щодо шахрайства.

9. На підставі опрацювання матеріалів кримінальних проваджень встановлено обов’язкові судові експертизи, що необхідно призначати під час розслідування шахрайства у сфері використання інтернет-банкінгу. Визначено окремі аспекти підготовки та проведення судових експертиз, а також об’єкти, які можуть бути направлені на експертизу.

Основні результати розділу опубліковано у працях [102; 103; 104].

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, що виявляється в розробленні теоретико-прикладних засад методики розслідування шахрайства у сфері використання інтернет-банкінгу, а також формулювання науково обґрунтованих практичних рекомендацій і пропозицій щодо їх розвитку й удосконалення. У результаті дослідження сформовано низку теоретичних положень, висновків і практичних рекомендацій, основними з яких є такі:

1. Здійснено криміналістичний аналіз розслідування шахрайства у сфері використання інтернет-банкінгу. Опрацювання ґенези наукових поглядів щодо побудови методики розслідування шахрайства у сфері використання інтернет-банкінгу дозволило виокремити в ній такі складові: 1) криміналістична характеристика шахрайства у сфері використання інтернет-банкінгу; 2) аналіз початкових відомостей та їх оцінка; 3) перелік обставин, що підлягають встановленню в кримінальному провадженні; 4) типові слідчі ситуації, які формуються під час розслідування шахрайства, а також алгоритми їх реалізації; 5) сукупність тактичних операцій для реалізації конкретних завдань розслідування; 6) взаємодія уповноважених осіб з окремими підрозділами Національної поліції та іншими державними органами в кримінальному провадженні; 7) профілактична діяльність уповноважених осіб у кримінальному провадженні; 8) тактика проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій на початковому етапі розслідування шахрайства; 9) тактика проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій на подальшому етапі розслідування шахрайства; 10) особливості використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу.

Виявлено фактори, що впливають на здійснення електронних операцій

у сфері використання інтернет-банкінгу. Доведено, що наявні ефективні заходи щодо запобігання шахрайським виявам не відповідають сучасним загрозам.

2. Схарактеризовано сучасні наукові підходи до розуміння сутності та системи криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. З'ясовано концептуальні засади формування криміналістичної характеристики шахрайства та запропоновано авторське визначення поняття криміналістичної характеристики.

На основі узагальнення матеріалів кримінальних проваджень окреслено структуру криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу, що охоплює такі складові: типові способи шахрайства (підготовка, безпосереднє вчинення, приховування), обстановка учинення шахрайських дій, слідова картина, особа злочинця (шахрая), особа потерпілого.

З'ясовано, що вказані елементи мають сталі кореляційні зв'язки й важливе значення для початкового етапу розслідування шахрайства та дозволяють невідкладно проводити слідчі (розшукові) дії та НСРД, вчасно висувати слідчі версії, вживати заходів щодо встановлення особи шахрая та його затримання.

3. Схарактеризовано основні елементи криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу.

Доведено, що *способи* протиправної діяльності мають досить широкі межі та виявляються в системі взаємопов'язаних дій із підготовки, безпосереднього вчинення та приховування шахрайських дій. Визначено найбільш типові способи безпосереднього вчинення шахрайства, зокрема: фішинг, спамінг і кардинг. З'ясовано та систематизовано способи підготовки та приховування протиправних діянь. Розкрито злочинні шахрайські схеми, які використовують під час дії запровадженого воєнного стану.

Визначено *обстановку* здійснення шахрайських дій. Доведено, що обстановка шахрайства визначається умовами часу й місця, які здебільшого

не мають чітких територіальних і часових меж.

Проаналізовано систему інформаційних даних щодо обстановки шахрайства у сфері використання інтернет-банкінгу на основі опрацювання просторово-часових, економічних, психологічних і соціальних факторів. Встановлено найбільш поширені місця вчинення шахрайських дій, а саме: місця розташування ЕОТ, що були використані під час учинення шахрайства (місце проживання або роботи підозрюваного, місця загального доступу) – 76 %; місця розміщення терміналів, банків, банкоматів та інших фінансових установ – 15 %; місця перебування особи потерпілого, на яку було спрямовано шахрайські дії, – 28 %.

Розглянуто *слідову картину*, а також встановлено кореляційні зв'язки між слідами та способами вчинення шахрайства у сфері використання інтернет-банкінгу. Доведено, що слідову картину шахрайства становлять три групи слідів – матеріальні, ідеальні та цифрові сліди. Особливу роль у слідовій картині відіграють цифрові (електронні, віртуальні) сліди, які здебільшого виявляють у таких місцях: а) профілях соціальних мереж (Facebook, Instagram, Twitter); б) месенджерах (Telegram, Viber); в) застосунках для переписок криптовалютного спрямування (Binance, OKX); г) кеш-пам'яті онлайн магазинів; д) базах інтернет-провайдерів тощо.

Окреслено криміналістично значущі ознаки *особи злочинця* (шахрая). Сформовано вірогідний «портрет» особи шахрая. Наголошено, що особам, які вчиняють шахрайства у сфері інтернет-банкінгу, притаманні високий рівень інтелекту й винахідливість.

Розглянуто структуру злочинної організації, яка вчиняє шахрайські дії у сфері використання інтернет-банкінгу, до якої належать такі групи осіб: організатори; адміністратори сайтів, де розміщуються неправдиві відомості про товари або надання послуг; продавці, які спілкуються з потенційними потерпілими; спамери; фішери; програмісти; хакери; охоронці; корумповані представники органів державної влади й управління, працівники правоохоронних органів, які беруть участь у прикритті організованої

злочинної діяльності.

Надано характеристику *особі потерпілого,* визначено й схарактеризовано віктимогенні групи потерпілих. Виокремлено віктимогенні групи осіб, стосовно яких було вчинено шахрайські дії.

4. Конкретизовано особливості початкового етапу розслідування шахрайства у сфері використання інтернет-банкінгу.

Виокремлено особливості аналізу й оцінки первинної інформації, а також визначено коло обставин, що підлягають встановленню в кримінальному провадженні. Зокрема, встановлено, що первинна інформація, яка слугувала підставою для внесення відомостей до ЄРДР, була одержана уповноваженими особами з таких джерел: а) заяви, листи й повідомлення, що надійшли від потерпілих від шахрайських дій, – 67 %; б) заяви, листи й повідомлення від громадян, які стали свідками вчинення шахрайських дій або одержали про них інформацію, – 14 %; в) звернення, заяви, листи й повідомлення від працівників фінансових установ різних форм власності – 9 %; г) матеріали справ, які було виокремлено з інших кримінальних проваджень, – 3 %; д) матеріали, одержані в межах реалізації НСРД або розшукових заходів, – 7 %.

Визначено сукупність обставин, що підлягають встановленню під час розслідування шахрайства у сфері використання інтернет-банкінгу, а саме: 1) обставини, що розкривають умови та способи вчинення шахрайства (інформація про час і місце його вчинення, відомості щодо способу підготовки, безпосереднього вчинення та приховування шахрайських дій, зокрема застосування спам-ботів, використання вірусних програм до ЕОТ потерпілих, використання різноманітних шахрайських схем), засоби, що використовували під час учинення шахрайських дій; 2) обставини, які характеризують особу злочинця або групу осіб (кількість шахраїв, схема розподілу між ними обов’язків, визначення їхньої ролі в злочинному угрупованні); 3) обставини, які характеризують особу потерпілого (віктимність її дій, базовий чи професійний користувач ЕОТ); 4) причиново-

наслідкові зв’язки між діями шахраїв і результатами, що їх характеризують; 5) встановлення причин та умов, що сприяли вчиненню шахрайських дій; 6) обставини, що обтяжують або пом’якшують покарання; 7) вид і розмір шкоди, яка завдана шахрайськими діями; 8) обставини, які є приводом для звільнення шахрая від кримінальної відповідальності.

5. Сформовано типові слідчі ситуації, що виникають під час розслідування шахрайства у сфері використання інтернет-банкінгу: вчинено шахрайські дії, наявна особистісна доказова база, злочинця (шахрая) встановлено – 27 %; здійснено шахрайські дії, є особистісна доказова база, злочинця (шахрая) не встановлено – 52 %; вчинено шахрайські дії, наявна особистісна та матеріальна доказова база, злочинця (шахрая) не встановлено – 16 %; вчинено шахрайські дії, повністю відсутня доказова база – 5 %. На основі узагальнення судово-слідчої практики запропоновано алгоритми вирішення наведених типових слідчих ситуацій, що виникають на початковому етапі розслідування.

Доведено, що вирішення слідчих ситуацій безпосередньо залежить від ефективної взаємодії слідчого з працівниками оперативних підрозділів Національної поліції, а також представниками органів державної влади та управління. Під час розслідування шахрайства у сфері використання інтернет-банкінгу особливого значення набуває «обмін інформацією» як одна з найбільш ефективних форм взаємодії, особливо в умовах запровадженого воєнного стану.

6. Конкретизовано особливості організації і тактики проведення процесуальних дій на початковому етапі розслідування шахрайства у сфері використання інтернет-банкінгу. На початковому етапі розслідування слідчому необхідно провести такі заходи: допит потерпілого, огляд ЕОТ потерпілого (комп’ютера, смартфона, планшета), огляд і долучення до справи фотографій або відеозаписів, розшук і встановлення особи шахрая, аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці (транспортному засобі, квартирі), візуальне

спостереження за особою, негласне зняття інформації з транспортних телекомунікаційних мереж, призначення експертизи тощо.

Запропоновано низку тактичних завдань, що мають бути реалізованими уповноваженими особами у кримінальному провадженні, а також розроблено комплекси дій для їх вирішення в межах проведення початкового та подальшого етапів розслідування, зокрема: 1) тактичне завдання «Профілактика протиправних дій» – реалізація відповідних профілактичних заходів для усунення причин та умов учинення шахрайства у сфері використання інтернет-банкінгу; 2) тактичне завдання «Встановлення шахрая» – проведення низки процесуальних дій і заходів, спрямованих на виконання вказаного завдання; 3) тактичне завдання «Встановлення співучасників в організованій групі чи злочинній організації» – з'ясування ймовірної участі та ролі шахрая в злочинному угрупованні.

7. Розкрито організаційно-тактичне забезпечення проведення процесуальних дій на подальшому етапі розслідування шахрайства у сфері використання інтернет-банкінгу. З'ясовано, що на цьому етапі розслідування в 100 % випадків коло підозрюваних встановлено.

Наведено безконфліктні та конфліктні ситуації *допиту підозрюваного*. Для вирішення конфліктних ситуацій доцільно використовувати низку тактичних прийомів допиту, серед яких ключове місце посідають встановлення психологічного контакту з підозрюваним, пред'явлення речових доказів (флеш-накопичувачі, скріншоти переписок із потерпілим, скріншоти із хмарних сховищ) і матеріалів кримінального провадження (протоколів допиту потерпілих та свідків, протоколів обшуку).

Запропоновано перелік питань, що необхідно з'ясувати під час допиту підозрюваного, а саме: 1) які способи застосовувалися для входу в застосунок інтернет-банкінгу (використання спам-ботів; реквізитів картки, одержаної від конкретного потерпілого шляхом шахрайських дій; використання реквізитів картки, отриманої з web-сторінок підставних інтернет-магазинів); 2) у який спосіб вчинено шахрайські дії (шляхом отримання доступу до ЕОТ з

паролями, що встановив потерпілий; шляхом використання мережі Wi-Fi); 3) чи вчинено шахрайські дії організованою групою або злочинною організацією; якщо так, то якою є структура злочинного угруповання; 4) який статус та обов'язки кожного зі співучасників шахрайства; 5) яким чином розподілялися викрадені майно та грошові кошти між співучасниками; 6) протягом якого проміжку часу було вчинено шахрайські дії; 7) наявність учинення супутніх кримінальних правопорушень; 8) які знаряддя й засоби використовувались під час учинення шахрайських дій (комп'ютери, смартфони, модеми, маршрутизатори, браузери, спам-боти); 9) якою є загальна сума грошових коштів, що була отримана шляхом реалізації шахрайських дій у сфері використання інтернет-банкінгу тощо.

Схарактеризовано організаційно-тактичне забезпечення проведення одночасного допиту двох або більше раніше допитаних осіб. З'ясовано/Доведено, що вказана процесуальна дія має бути спрямована на усунення невідповідностей у показаннях раніше допитаних осіб, зокрема: 1) підозрюваного та потерпілого (87 %) – як було вчинено шахрайські дії; що було застосовано засоби для їх учинення (комп'ютер, планшет, ноутбук, смартфон) тощо; 2) між підозрюваними (9 %) – які саме ролі в організованій групі чи злочинній організації вони виконували тощо; 3) підозрюваного та свідка (2 %); 4) потерпілого та свідка (1 %); 5) між потерпілими (1 %).

Акцентовано увагу на обов'язковій реалізації пред'явлення підозрюваного для впізнання за фотографією та голосом. Надано перелік місць, де необхідно проводити обшук.

8. Визначено особливості використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу.

Серед основних форм використання спеціальних знань у кримінальному провадженні виокремлено такі: а) безпосереднє застосування уповноваженою особою спеціальних знань під час реалізації окремих слідчих (розшукових) дій, НСРД та інших процесуальних і розшукових заходів; б) залучення спеціаліста до проведення окремих слідчих (розшукових) дій,

НСРД та інших процесуальних дій і розшукових заходів; в) консультативна допомога спеціаліста; г) призначення та проведення судових експертиз.

Надано пропозиції щодо внесення змін до ч. 1 ст. 71 КПК України, яку запропоновано викласти в такій редакції: «Спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками, що можуть бути застосовані під час досудового розслідування та судового розгляду шляхом надання довідок, пояснень, консультацій і висновків в усній чи письмовій формі для вирішення питань, що вимагають володіння відповідними спеціальними знаннями чи навичками».

На підставі узагальнення матеріалів кримінальних проваджень запропоновано обов'язкові судові експертизи, що необхідно призначати під час розслідування шахрайства у сфері використання інтернет-банкінгу, а саме: а) судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів, експертиза цифрової інформації, програмно-комп'ютерна експертиза); б) судово-бухгалтерська експертиза; в) інформаційно-комп'ютерна експертиза; г) експертиза телекомунікаційних систем і засобів.

Визначено окремі аспекти підготовки та проведення судових експертиз, а також об'єкти, що можуть бути направлені на експертизу.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Аленін Ю. П. Початок досудового розслідування за КПК України 2012 р. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 199–208.

2. Анапольська А. І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : автореф. дис. … канд. юрид. наук: спец. : 12.00.09. Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. Луганськ, 2011. 238 с.

3. Анапольська А. І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. … канд. юрид. наук: спец. : 12.00.09 / Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. Луганськ, 2011. 238 с.

4. Антонюк О. А. Наукова полеміка щодо сутності методики розслідування кримінальних правопорушень проти громадського порядку. *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. 249–252.

5. Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монограф. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

6. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. … на здобуття наук. ступеня канд. юрид. наук: 12.00.09. Київський національний університет імені Тараса Шевченка. Київ, 2008. 20 с.

7. Бородай О. В. Особа злочинця як елемент криміналістичної характеристики несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Вісник ЛДУВС*

ім. Е. О. Дідоренка. 2018. Вип. 4 (84). С. 212–220.

8. Варцаба В. М. Розслідування злочинів, що вчиняються організованими злочинними групами (тактико-психологічні основи) : монографія / за наук. ред. В. Ю. Шепітька. Харків : Ериф, 2004. 111 с.

9. Весельський В. К., Зав'ялов С. М., Пясковський В. В. Сучасні можливості використання даних про спосіб учинення злочину в боротьбі зі злочинністю : навч. посіб. [для студ. вищ. навч. закл.]. Київ : КНТ, 2009. 160 с.

10. Вискарка Т. В. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2021. Випуск 2. Том 2. С. 105–110.

11. Волобуєв А. Ф. Криміналістична характеристика розкрадань майна у сфері підприємницької діяльності. *Вісник Університету внутрішніх справ*. 1997. Вип. 2. С. 26–37.

12. Говорова К. І. Місце судово-економічної експертизи у протидії шахрайствам з надання послуг у банківській сфері через інтернет. *Теорія та практика судової експертизи і криміналістики*. 2020. № 22. С. 461–472.

13. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : автореф. дис. … канд. юр. наук : 12.00.09. Харківський національний університет внутрішніх справ. Харків, 2008. 216 с.

14. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юр. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2008. 216 с.

15. Головкін С. В. Предмет шахрайства відносно особи в сучасних умовах. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2008. Спеціальний випуск № 5, частина 3. С. 185–193.

16. Дуда Х. І. Поняття комп'ютерних слідів злочину. *Науковий вісник*

Національного університету біоресурсів і природокористування України. 2014. Вип. 197. Ч. 1. С. 262–267.

17. Єфімов М. М. Криміналістична характеристика як елемент методики розслідування кримінальних правопорушень проти моральності. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 3. С. 161–167.

18. Єфімов М. М. Методика розслідування кримінальних правопорушень проти моральності : наукові та праксеологічні основи : монографія. Одеса : Видавничий дім «Гельветика», 2020. 392 с.

19. Єфімов М. М. Розслідування злочинів проти громадського порядку та моральності : навч. посібник. 2-е вид., доп. і перероб. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 188 с.

20. Єфімов М. М., Пиріг І. В. Методика розслідування окремих видів кримінальних правопорушень : підручник. Дніпро : Видавець Біла К. О., 2022. 271 с.

21. Єфімов М. М., Чаплинський К. О., Жилін А. Е. Методика розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Видавництво «Юридика», 2024. 218 с.

22. 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. Серія ПРАВО. Випуск 32. Том 3. С. 117–121.

23. Жилін А. Е. Наукова полеміка відносно опису ознак та властивостей окремих елементів криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2023. Випуск 1. С. 89–94.

24. Жилін А. Е. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : автореф. дис. канд. юрид. наук : 12.00.09. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 20 с.

25. Жилін А. Е. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : дис. … канд. юрид. наук : 12.00.09 /Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 226 с.

26. Журавель В. А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом : науково-практичний посібник. Харків : ТОВ «Одіссей», 2005. 112 с.

27. Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : автореф. дис. … канд. юрид. наук : 12.00.09. Національна академія внутрішніх справ України. Київ, 2005. 20 с.

28. 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.

29. Заяць К. Д. Методика розслідування шахрайств : автореф. дис. … канд. юрид. наук : 12.00.09. Харківський нац. ун-т внутр. справ. Харків, 2020. 20 с.

30. Заяць К. Д. Методика розслідування шахрайств : дис. … канд. юрид. наук : 12.00.09 / Харківський нац. ун-т внутр. справ. Харків, 2020. 196 с.

31. Заяць К. Д. Особливості встановлення способу шахрайства на стадії досудового розслідування. *Актуальні проблеми кримінального процесу та криміналістики* : тези доп. Міжнар. наук.-практ. конф. (м. Харків, 29 жовт. 2021 р.). Харків : ХНУВС, 2021. С. 155–158.

32. Заяць К. Д. Особливості сучасних форм вчинення шахрайств та їх криміналістичне значення. *Підприємництво, господарство і право*. 2017. № 11. С. 207–210.

33. Іванов Ю. Ф., Джужа О. М. Кримінологія : навч. посіб. Київ : Вид. Паливода А. В., 2006. 264 с.

34. Коба В. Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2024. 266 с.

35. Коваленко І. О. Деякі аспекти проведення допиту потерпілого при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Процесуальне та техніко-криміналістичне забезпечення досудового розслідування* : матеріали Всеукраїнської науково-практичної конференції (м. Харків, 28 лист. 2019 р.). Харків : Харків. нац. ун-т внутр. справ, 2019. С. 84–86.

36. Коваленко І. О. Деякі аспекти проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Правове життя сучасної України : у 3 т.* : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. Т. 3. С. 385–387.

37. Коваленко І. О. Деякі аспекти проведення огляду місця події при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Актуальні проблеми забезпечення публічного порядку та безпеки в сучасних умовах : вітчизняний та міжнародний досвід :* матеріали Міжнар. наук.-практ. конф. (Дніпро, 25 жовт. 2019 р.). Дніпро : ДДУВС, 2019. С. 123–125.

38. Коваленко І. О. До питання криміналістичної характеристики шахрайства в сфері банківських електронних платежів. *Актуальні проблеми експертного забезпечення досудового розслідування* : матеріали наук.-практ. семінару (м. Дніпро, 29 трав. 2020 р.). Дніпро : Дніпропетровський державний університет внутрішніх справ, 2020. С. 77–79.

39. Коваленко І. О. Криміналістичний аналіз шахрайства у сфері банківських електронних платежів. *Прикарпатський юридичний вісник.* 2020. № 5 (34). С. 137–140.

40. Коваленко І. О. Обставини, що підлягають встановленню під час

розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник.* 2021. № 1 (36). С. 98–101.

41. Коваленко І. О. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право.* 2020. № 12 С. 262–266.

42. Коваленко І. О. Окремі питання визначення обставин, що підлягають встановленню при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Актуальні проблеми криміналістики та судової експертизи*: матеріали наук.-практ. семінару (м. Дніпро, 28 трав. 2021 р.). Дніпро: Дніпр. держ. ун-т внутр. справ, 2021. С. 145–147.

43. Коваленко І. О. Організаційно-практичне забезпечення проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2019. № 6. С. 117–122.

44. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … докт. філософії за спеціальністю – 081 Право / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2022. 234 с.

45. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights»*. 2020. № 1. С. 99–103.

46. Когутич І. І Окремі питання сутності та форм використання спеціальних знань у кримінальному провадженні. *Вісник Академії адвокатури України.* 2015. Т. 12. Ч. 2 (33). С. 112–123.

47. Коршикова Т. В Алгоритм дій слідчого з розслідування шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні питання криміналістики* : матеріали Всеукр. наук.-практ.

конф. (м. Київ, 20 груд. 2019 р.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2019. С. 368–370.

48. Коршикова Т. В. Обставини, які підлягають доказуванню під час вчинення шахрайств з використанням електронно-обчислювальної техніки. *Кримінальний процес та криміналістика : сучасний стан та перспективи:* тези доп. Всеукр. наук.-практ. конф. (Харків, 26 лист. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. С. 313–315.

49. Коршикова Т. В. Особливості підготовчого етапу проведення обшуку при розслідуванні шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні проблеми кримінального права, процесу та криміналістики та оперативно-розшукової діяльності :* тези доп. IV Всеукр. наук.-практ. конф. (Хмельницький, 26 лют. 2021 р.) / Нац. акад. Держ. прикордон. служби. Хмельницький : Вид-во НАДПСУ, 2021. С. 520–522.

50. Коршикова Т. В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет. *Молодий вчений*. 2016. № 1 (28). Ч. 2. С. 51–54.

51. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філософії : 081 – Право / Національна академія внутрішніх справ. Київ, 2021. 255 с.

52. Коршикова Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. С. 129–135.

53. Коршикова Т. В. Стан наукових досліджень проблем розслідування шахрайств учинених із використанням електронно-обчислювальної техніки. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2020. Вип. 3 (91). С. 286–294.

54. Коршикова Т. В. Типові слідчі ситуації та програми дій слідчого на початковому етапі розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки. *Південноукраїнський правничий*

часопис. 2020. Вип. 4. С. 123–131.

55. Коршикова Т. В. Форми використання спеціальних знань при розслідуванні шахрайства, вчиненого із використанням мережі Інтернет. *Актуальні проблеми кримінального права* : тези доп. XI Всеукр. наук.-теорет. конф., присвяч. пам'яті проф. П. П. Михайленка (Київ, 20 листоп. 2020 р.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2020. С. 296–298.

56. Коршикова Т. В., Бишевець О. В. Особа злочинця як елемент криміналістичної характеристики шахрайств, що вчиняються в мережі Інтернет. *Вісник кримінального судочинства*. 2016. № 1. С. 81–87.

57. Криміналістика : навч. посіб. / за заг. ред. Є. В. Пряхіна. Київ : Атіка, 2012. 496 с.

58. Криміналістика : підруч. для студ. вищ. навч. закл. / Чаплинський К. О. та інші. Дніпро : Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2017. 419 с.

59. Криміналістика : підручник / за заг. ред. В. В. Пясковського. 2-ге вид., перероб. і допов. Харків : Право, 2020. 752 с.

60. Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

61. Криміналістика : підручник / за ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і доп. Харків : Право, 2008. 464 с.

62. Криміналістика : підручник / Кол. авторів; керівник В. Ю. Шепітько. Київ : Видавничий Дім «Ін Юре», 2001. 546 с.

63. Криміналістика : підручник : у 2 т. Т. 2 / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 312 с.

64. Кримінальний кодекс України від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення – 13.02.2024).

65. Кримінальний процесуальний кодекс України від 13.04.2012 р.

№ 4651-VIII. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення – 14.02.2024)

66. Кримінологія : Загальна та Особлива частини : [підручник] / [І. М. Даньшин, В. В. Голіна, М. Ю. Валуйська та ін.] ; за заг. ред. В. В. Голіни. 2-ге вид. перероб. і доп. Харків : Право, 2009. 288 с.

67. Кузьмічов В. С., Прокопенка Г. І. Криміналістика : навч. посіб. / За заг. ред. В. Г. Гончаренка та Є. М. Моісєєва. Київ : Юрінком Інтер, 2001. 368 с.

68. Курило В. І., Михайлов О. Є., Яра О. С. Кримінологія : Загальна частина. Курс лекцій / Київ : Кондор, 2006. 192 с.

69. Лазебний А. М., Левицький Б. С. Криміналістичне забезпечення розслідування організованої злочинності. *Міжнародний юридичний вісник : актуальні проблеми сучасності (теорія та практика)*. 2019. Вип. 14. С. 189–198.

70. Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій. *Lex Portus*. 2019. № 1 (15). С. 89–101.

71. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю. *Право і безпека*. 2017. № 1. С. 85–89.

72. Логінова В. В. Поняття та значення особи злочинця в методиці розслідування тілесних ушкоджень. *Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах* : Матер. Міжнар. наук.-практ. конф. (м. Запоріжжя, 5 листоп. 2010 р.). у 2-х ч. Ч. 1. Запоріжжя : ЗЮІ ДДУВС, 2010. С. 115–118.

73. Луговий В. О. Наукові диспути стосовно формулювання поняття «транснаціональне організоване злочинне угруповання». *Науковий вісник публічного та приватного права*. 2023. Випуск 6. С. 198–202.

74. Лужецька О. Р. Особа злочинця як елемент криміналістичної характеристики вимагання, пов’язаного із застосуванням насильства над потерпілим. *Науковий вісник Національного університету Державної*

податкової служби України (економіка, право). 2013. № 4. С. 196–201.

75. Лук'янчиков Б. Є., Лук'янчиков Є. Д., Петряєв С. Ю. Криміналістика : Навчальний посібник для студ. юрид. спец. вищ. навч. закл. в двох частинах. Частина II : Криміналістична тактика. Методика розслідування. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського. 2017. 505 с.

76. Макаренко Є І., Негодченко О. В., Тертишник В. М. Експертизи на досудовому слідстві : навчальний посібник. Дніпропетровськ : Дніпроп. юрид. ін-т МВС України, 2001. 204 с.

77. Малій М. О. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження : дис. … докт. філософії : 081 – Право / Хмельницький, 2023. 224 с.

78. Малярова В. О. Тактико-криміналістичні та процесуальні основи пошуку та затримання злочинця : дис. … канд. юрид. наук : 12.00.09 / Нац. ун-т внутр. справ. Харків, 2005. 238 с.

79. Мамедова Л. Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів : міжнародний досвід. *Юридичний науковий електронний журнал.* 2021. № 1. С. 392–395. URL : http://www.lsej.org.ua/12_2021/100.pdf (дата звернення – 12.01.2024).

80. Мельниченко С. П. Криміналістична характеристика та особливості розслідування незаконного переміщення вогнепальної зброї : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2016. 223 с.

81. Миргородський О. І. Детермінанти шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Юридичний науковий електронний журнал*. 2021. № 9. С. 452–454.

82. Миргородський О. І. Досвід Естонської Республіки в частині регулювання кримінальної відповідальності за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Юридична наука*. 2020. № 3. Том 2. С. 131–135.

83. Миргородський О. І. Широкомасштабна війна російської федерації проти України як детермінант поширення шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Реформування українського законодавства : проблемні питання та шляхи їх вирішення :* матеріали міжнародної науково-практичної конференції (м. Київ, 07–08 лютого 2024 р.). Київ : Науково-дослідний інститут публічного права, 2024. С. 171–173.

84. Мізерак А. Б. Шахрайство при інтернет-торгівлі : схеми та аспекти запобігання. *Маркетинг і контролінг : сучасні виклики підприємництв,* Київ, 2017. С. 153–155.

85. Мойсик В. Р. Проблеми кримінальної відповідальності за шахрайство з фінансовими ресурсами : дис. … канд. юрид.наук : 12.00.08 / Київський національний університет імені Тараса Шевченка. Київ, 2002. 222 с.

86. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : автореф. дис. … канд. юрид.наук : 12.00.09. Національна юридична академія України імені Ярослава Мудрого. Харків, 2007. 19 с.

87. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : дис. … канд. юрид.наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2007. 266 с.

88. Назаренко К. Ю. Розслідування злочинів, пов’язаних зі створенням або утриманням місць розпусти і звідництвом : дис. … к-та юр. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2016. 218 с.

89. Некрасов В. Атака по телефону : Україну накрила хвиля кібершахрайства. URL : https://www.epravda.com.ua/rus/publications /2017/01/30/619178/ (дата звернення – 12.01.2024)

90. Нізовцев Ю. Ю., Омельян О. С. Щодо підготовки та призначення судових експертиз у межах розслідування кримінальних правопорушень, пов’язаних із кібератаками. *Криміналістичний вісник*. 2021. № 2 (36). С. 59–

68.

91. Одерій О. В. Теорія і практика розслідування злочинів проти довкілля монографія. Харків : Діса плюс, 215. 528 с.

92. 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.

93. Павлова Н. В. Особливості розслідування шахрайства, пов'язаного з відчуженням приватного житла : дис... канд. юрид. наук: 12.00.09 / Дніпропетровський держ. ун-т внутрішніх справ. Дніпропетровськ, 2007. 223 с.

94. Павлова Н. В., Птушкін Д. А., Чаплинський К. О. Теоретичні засади методики розслідування шахрайства, пов’язаного з відчуженням об’єктів нерухомого майна громадян : монографія. Дніпр. державний університет внутрішніх справ. Херсон : Видавничий дім «Гельветика», 2019. 196 с.

95. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп’ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2007. 228 с.

96. Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

97. Перхун С. О. До питання визначення обставин, які підлягають встановленню під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення* : матеріали Міжнар. наук.-практ. конф. (Київ, 13–14 берез. 2023 р.). Київ : Наук.-дослід. ін-т публіч. права, 2023. С. 131–133.

98. Перхун С. О. Криміналістична характеристика організованих

груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200.

99. Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

100.Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

101.Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

102.Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової системи України* : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123.

103.Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

104.Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу : теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

105.Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу : наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342.

(Республіка Польща).

106.Попов К. Л. Соціально-психологічні орієнтири у віктимологічному дослідженні жертви шахрайства. *Наукові праці Національного авіаційного університету*. Серія : Юрид. вісник «Повітряне і космічне право»: зб. наук. пр. Київ : НАУ, 2015. № 1 (34). С. 164–169.

107.Попова І. М. Розслідування шахрайств, пов'язаних із залученням коштів громадян на будівництво житла : дис. … к.ю.н. : 12.00.09 / Національна академія внутрішніх справ. Київ, 2011. 250 с.

108.Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 січ. 1998 р. № 53/5. URL : https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення – 23.01.2024).

*109.*Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 1993 р. URL : https://zakon.rada.gov.ua/laws/show/3341-12#Text (дата звернення – 12.12.2023)

110.Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південноукраїнський правничий часопис.* 2018. № 2. С. 30–33.

111.Птушкін Д. А. Розслідування шахрайства, вчиненого щодо об'єктів нерухомого майна громадян : дис. ... к.ю.н. : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 240 с.

112.Птушкін Д. А. Щодо елементів, які визначають індивідуальність типової слідчої ситуації у справах про шахрайства відносно об'єктів нерухомості громадян. *Актуальні проблеми розслідування злочинів в сучасних умовах* : матеріали Всеукраїнської наук.-практ. конференції з нагоди святкування 10-річчя факультету підготовки фахівців для підрозділів слідства (м. Дніпропетровськ, 24 верес. 2015 р.). Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ, 2015. С. 124–127.

113.Пчеліна О. В. Теоретичні основи формування та реалізації методики розслідування злочинів у сфері службової діяльності : монографія. Харків : ТОВ «В справі», 2017. 524 с.

114.Рейнгольд А. В. Концептуальні підходи до побудови криміналістичної характеристики шахрайства в інтернет-комерції. *Юридична наука*. 2019. № 6. Том 2. С. 73–77.

115.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.

116.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.

117.Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : автореф. дис. … канд. юрид.наук : 12.00.09. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 20 с.

118.Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : дис. … канд. юрид.наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 250 с.

119.Рейнгольд А. В. Оцінка первинної інформації на початку розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 1. Том 2. С. 114–118.

120.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.

121.Рейнгольд А. В. Типові слідчі ситуації під час розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 2. Том 2. С. 129–133.

122.Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. … к-та юр. наук : 12.00.09. Національна юридична академія України імені Ярослава Мудрого. Харків, 2009. 19 с.

123.Салтевський М. В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навч. посіб. Харків : Нац. юрид акад. України, 2000. 35 с.

124.Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

125.Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ : КНТ, 2009. 328 с.

126.Самойлов С. В. Про необхідність володіння захиснику певними спеціальними знаннями при участи у справах про шахрайства, учинених з використанням мережі «Інтернет». *Захисник у кримінальному процесі* : матеріали міжнар. наук.-практ. конф. (м. Донецьк, 10 лютого 2012 р.). Донецьк : Донецький університет економіки і права, 2012. С. 93–94.

127. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юр. наук : 12.00.09 / Донецький юридичний інститут МВС України. Донецьк, 2014. 18 с.

128.Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юр. наук : 12.00.09 / Донецький юридичний інститут МВС України. Донецьк, 2014. 226 с.

129.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.

130.Самойлов С. В., Одерій О. В. Застосування спеціальних знань під час розслідування шахрайств, учинених з використанням мережі Інтернет.

Криміналістичний вісник. 2012. № 2 (18). С. 106–113.

131.Сенаторов М. В. Потерпілий від злочину в кримінальному праві / За науковою редакцією доктора юридичних наук, професора, академіка Академії правових наук України В. І. Борисова. Харків : Право, 2006. 208 с.

132.Сисолятін В. В. Актуальні питання опису ознак та властивостей окремих елементів криміналістичної характеристики правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2023. Випуск 5. С. 151–156.

133.Сисолятін В. В. Криміналістична характеристика особи, яка вчиняє кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 13-14 березня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 31–33.

134.Сисолятін В. В. Наукові підходи стосовно типових слідчих ситуацій при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 129–133 (Республіка Польща).

135.Сисолятін В. В. Наукова полеміка з приводу обставин, що підлягають встановленню при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2023. Випуск 4. С. 123–223.

136.Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид.наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2024. 232 с.

137.Справа № 200/12729/18. Архів Бабушкінського районного суду м. Дніпропетровська, 2021 р.

138.Справа № 201/524/23. Архів Жовтневого районного суду м. Дніпро, 2023 р.

139.Справа № 296/1022/19. Архів Корольовського районного суду м. Житомира, 2019 р.

140.Справа № 333/1359/22. Архів Комунарського районного суду м. Запоріжжя, 2022 р.

141.Справа № 334/1256/21. Архів Ленінського районного суду м. Запоріжжя, 2021 р.

142.Справа № 335/1939/21. Архів Орджонікідзевського районного суду м. Запоріжжя, 2022 р.

143.Справа № 405/5286/20. Архів Ленінського районного суду м. Кіровограда, 2021 р.

144.Справа № 554/1839/21. Архів Октябрського районного суду м. Полтави, 2021 р.

145.Справа № 672/697/23. Архів Городоцького районного суду Хмельницької обл., 2023 р.

146.Справа № 686/5430/23. Архів Хмельницького міськрайонного суду Хмельницької обл., 2023 р.

147.Справа № 752/12644/23. Архів Голосіївського районного суду м. Києва, 2023 р.

148.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.

149.Судова бухгалтерія / за ред. В. М. Глібка, О. П. Бущана. Київ : Юрінком Інтер, 2004. 224 с.

150.Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : автореф. дис. … д-ра юрид. наук : 12.00.09. Національна юридична академія України імені Ярослава Мудрого. Харків, 2003. 34 с.

151.Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеська національна юридична академія. Одеса : Фенікс, 2007. 260 с.

152.Чаплинський К. О. Тактика пред'явлення для впізнання : навчально-методичний посібник. Дніпропетровськ : Дніпропетровський державний університет внутрішніх справ, 2007. 103 с.

153.Чаплинський К. О. Тактика проведення окремих слідчих дій : монографія. Дніпропетровськ : Ліра ЛТД, 2006. 416 с.

154.Чаплинський К. О. Тактичне забезпечення проведення слідчих дій : монограф. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2010. 560 с.

155.Чаплинський К. О. Тактичне забезпечення розслідування злочинів, вчинених злочинними угрупованнями : монографія. Дніпропетровськ : Дніпропетровський державний університет внутрішніх справ. 2009. 401 с.

156.Чаплинський К. О., Мінка П. Я. Розслідування злочинів, вчинених злочинними угрупованнями : навчальний посібник. Дніпропетровськ : Видавництво «Свідлер А.Л.», 2009. 225 с.

157.Чернявський С. С. Методика розслідування злочинів у сфері банківського кредитування : дис. … к.ю.н. : 12.00.09 / Національна академія внутрішніх справ України. Київ, 2001. 309 с.

158.Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. … доктора юр. наук : 12.00.09. Національна академія внутрішніх справ. Київ, 2010. 36 с.

159.Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : дис. … д-ра юрид. наук : спец. 12.00.09 / Національна академія внутрішніх справ. Київ, 2010. 610 с.

160.Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів : монографія. Вінниця : ТОВ «Нілан-ЛТД», 2017. 492 с.

161.Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів : наукові засади та напрями реалізації. *Сучасні тенденції розвитку криміналістики та кримінального процесу* : тези доп. міжнар. наук.-практ. конф. до 100-річчя від дня народження проф. М. В. Салтевського (м. Харків,

08 листоп. 2017 р.). МВС України. Харків. нац. ун-т внутр. справ. Харків, 2017. С. 220–222.

162.Чучко С. В. Використання спеціальних знань при розслідуванні шахрайств при купівлі-продажу товарів через мережу Інтернет. *Право і суспільство.* 2021. № 2. С. 234–240.

163.Чучко С. В. До питання взаємодії слідчих та оперативних підрозділів при розслідуванні шахрайства за фактом купівлі-продажу товарів через мережу Інтернет. *Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного забезпечення безпеки України та світу* : матеріали Міжнародної науково-практичної конференції (27 лист. 2020 р., м. Дніпро). Дніпро : Дніпр. держ. ун-т внутр. справ, 2020. С. 202–205.

164.Чучко С. В. Криміналістичний аналіз шахрайств, пов’язаних із куплею-продажем товарів через мережу Интернет. *Актуальні проблеми експертного забезпечення досудового розслідування* : матеріали регіонального науково-практичного семінару (31 травня 2020 р., м. Дніпро). Дніпро : Дніпр. держ. ун-т внутр. справ, 2020. С. 351–353.

165.Чучко С. В. Обставини, що підлягають встановленню при розслідуванні шахрайства, пов’язаного із торгівлею через мережу Інтернет. *Кібербезпека в Україні: правові та організаційні питання* : матеріали міжнародної науково-практичної конференції (26 лист. 2020 р., м. Одеса). Одеса : Одеський державний університет внутрішніх справ, 2020. С. 95–96.

166.Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філософії : 081 – Право / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 276 с.

167.Чучко С. В. Щодо регулювання правовідносин у віртуальному просторі при купівлі-продажу товарів через мережу Інтернет. *Вісник Національного технічного університету України «Київський Політехнічний Інститут». Політологія. Соціологія. Право*. № 1 (45). 2020. С. 78–82.

168.Шепітько В. Ю. Особа потерпілого в системі криміналістичної характеристики злочинів. *Проблеми законності* : республік. між від. наук. зб. / відп. ред. В. Я. Тацій. Харків : Нац. юрид. акад.. України, 2008. Вип. 93. С. 168–174.

169.Шеремет А. П. Криміналістика : навч. посіб. для студ. вищ. навч. закл. 2-ге вид. Київ : Центр учбової літ., 2009. 472 с.

170.Яремчук В. О. Криміналістичні та спеціальні знання при розслідуванні кримінальних правопорушень у банківській сфері**.** *Юридичний науковий електронний журнал*. 2022. № 6. С. 456–458.

171.Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України. *Економіка і суспільство.* 2018. Вип. 18. С. 836–842.

172.Chuchko, Sergey Fraud methods, related to purchase of goods through the Internet. *Науковий журнал «Visegrad Journal on Human Rights»*. 6 (volume 3) 2019. С. 234–238.

173.Sysoliatin, Valerii The further stage of the investigation of criminal offences involving internet banking (issues of concern). *Entrepreneurship, Economy and Law*. 2023. № 6. pp. 89–94.

174.Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

ДОДАТКИ

Додаток А

Зведені результати опитувань

227 працівників органів досудового розслідування, 142 працівника підрозділів дізнання, 224 співробітника оперативних підрозділів, 47 представників кіберполіції Національної поліції України, 88 працівників органів прокуратури та 71 працівник різних НДЕКЦ МВС України

	З а п и т а н н я	**%**
1.	**Вкажіть Ваш вік:**	
	До 25 років	**39**
	25-30 років	**30**
	31-40 років	**23**
	41 рік і старше	**8**
2.	**Вкажіть стаж практичної роботи:**	
	до 1 року	**7**
	від 1 до 3 років	**22**
	від 3 до 5 років	**32**
	від 5 до 10 років	**27**
	більше 10 років	**12**
3.	**Чи розслідували Ви або брали участь у розслідуванні шахрайства у сфері використання інтернет-банкінгу:**	
	так	**100**
	ні	**0**
4.	**Чи мали місце у Вашому підрозділі випадки розслідування шахрайства у сфері використання інтернет-банкінгу, та чи можете Ви надати інформацію з цього приводу:**	
	так	**100**
	ні	**0**
5.	**Чи розслідували Ви особисто або брали участь у розслідуванні шахрайства у сфері використання інтернет-банкінгу:**	
	так	**59**
	ні	**41**
6.	**Чи вважаєте Ви, що розслідування кримінальних правопорушень цієї/зазначеної категорії потребує відповідної кваліфікації уповноваженої особи у цьому напряму:**	
	так	**97**
	ні	**3**
7.	**Чи згодні Ви з твердженням щодо необхідності розроблення криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу, у питанні докладної побуди кореляційних зв'язків між окремими її елементами:**	

	так	**96**
	ні	**4**
8.	**На Вашу думку, якими чинниками зумовлено низьку якість розслідування кримінальних проваджень досліджуваної категорії та незначна кількість викритих і притягнутих до відповідальності злочинців:**	
	відсутність чіткої взаємодії й належної координації окремих підрозділів Національної поліції (зокрема, співробітників кіберполіції та слідчих)	**78**
	невчасне здійснення СРД, НСРД та інших процесуальних заходів	**59**
	поверхневе використання техніко-криміналістичних засобів під час проведення окремих процесуальних дій та ігнорування залучення відповідних спеціалістів	**78**
	відсутність міжнародної практики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу	**87**
	порушення послідовності дій під час збирання доказів на початковому етапі кримінального провадження	**73**
9.	**Назвіть тактичні помилки, що їх допускають/допущені уповноважені/-ними особи/-ами під час розслідування шахрайських дій:**	
	недотримання правильного порядку реалізації СРД, НСРД та інших розшукових заходів	**68**
	прорахунки в аналізі шахрайських дій на початковому етапі розслідування	**64**
	здійснення невідкладних СРД без участі відповідного спеціаліста	**61**
	неправильне визначення подальших напрямів кримінального провадження	**54**
	поверхневе проведення невідкладних СРД (огляд місця події, огляд ЕОТ)	**57**
10.	**Назвіть тактичні помилки, що їх допускають/допущені уповноважені/-ними особи/-ами під час розслідування шахрайських дій:**	
	недотримання правильного порядку реалізації СРД, НСРД та інших розшукових заходів	**68**
	прорахунки в аналізі шахрайських дій на початковому етапі розслідування	**64**
	здійснення невідкладних СРД без участі відповідного спеціаліста	**61**
	неправильне визначення подальших напрямів кримінального провадження	**54**
	поверхневе проведення невідкладних СРД (огляд місця події, огляд ЕОТ)	**57**
10.	**Чи виникають під час допиту підозрюваного в досліджуваній категорії кримінальних проваджень конфліктні ситуації:**	
	так	**21**

	ні	**79**
11.	**Назвіть, будь ласка, ситуації, що виникали під час проведення допиту підозрюваного при розслідуванні шахрайства у сфері використання інтернет-банкінгу:**	
	підозрюваний добровільно надає інформацію про обставини шахрайських дій, конфліктна ситуація відсутня	**21**
	підозрюваний викладає відомості про обставини вчинення шахрайських дій, але не пояснює її у повному об'ємі	**7**
	підозрюваний не надає повні та правдиві покази	**29**
	підозрюваний цілком відмовляється від комунікації з уповноваженою особою та від дачі свідчень	**34**
	підозрюваний не спростовує факт і зміст шахрайських дій, але спростовує свою участь у їх скоєнні	**9**
12.	**Які, на Вашу думку, найбільш доцільні тактичні прийоми під час проведення допиту підозрюваного при розслідуванні шахрайства у сфері використання інтернет-банкінгу:**	
	встановлення психологічного контакту	**96**
	застосування фактора раптовості	**61**
	створення уявлення про інформованість уповноваженої особи	**91**
	пред'явлення речових доказів та матеріалів справи	**29**
	зміна темпу допиту (зі швидкого на повільний та навпаки)	**47**
	створення напруги	**72**
	використання відеозапису	**38**
13.	**Назвіть, будь ласка, головні форми використання спеціальних знань під час розслідування досліджуваної категорії протиправних діянь:**	
	безпосереднє застосування уповноваженою особою спеціальних знань під час реалізації окремих слідчих (розшукових) дій, НСРД та інших процесуальних і розшукових заходів	**92**
	залучення спеціаліста до проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій і розшукових заходів	**85**
	консультативна допомога спеціаліста	**89**
	призначення та проведення судових експертиз	**100**
14.	**На Вашу думку, які чинники впливають на розповсюдження шахрайства у сфері використання інтернет-банкінгу?**	
	недосконалість законодавства у сфері інформаційних відносин	**81**
	недосконалість державного контролю за сферою використання інтернет-банкінгу	**53**
	брак ефективної взаємодії правоохоронних органів між собою	**58**
	віктимна поведінка (недбалість, необізнаність, зайва довірливість тощо) потерпілих	**97**
	інше	**46**

Додаток Б

Результати вивчення матеріалів

236 кримінальних проваджень із проблематики дослідження (ч.ч. 2-4 ст. 190 КК України) у таких областях: Вінницька, Дніпропетровська, Закарпатська, Запорізька, Івано-Франківська, Київська, Кіровоградська, Львівська, Миколаївська, Одеська, Полтавська, Сумська, Тернопільська, Харківська, Хмельницька, Чернігівська та Черкаська області, м. Київ.

№	Досліджувані питання	%
	КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА	
1	**Обстановка вчинення кримінального правопорушення**	
	1.1. Місце вчинення протиправних дій	
	1) місця розташування ЕОТ, що були використані під час учинення шахрайства (місце проживання або роботи підозрюваного, місця загального доступу)	**76**
	2) місця розміщення терміналів, банків, банкоматів та інших фінансових установ	**15**
	3) місця перебування особи потерпілого, на яку були спрямовані шахрайські дії	**28**
2	**Способи вчинення шахрайства у сфері використання інтернет-банкінгу**	
	2.1. Повноструктурний	**100**
	2.2. Підготовка до вчинення	**100**
	1) підбір необхідної ЕОТ (комп'ютер, смартфон, ноутбук)	**94**
	2) підготовка спам-ботів для їх застосування під час використання е-банкінгу потерпілими	**19**
	3) створення відповідного програмного забезпечення (вірусних програм)	**8**
	4) підбір групи осіб, стосовно яких буде вчинено шахрайські дії	**87**
	5) підготовка необхідної обстановки для вчинення шахрайських дій	**69**
	6) підбір співучасників для здійснення шахрайських дій	**34**
	7) розподіл ролей між ними	**28**
	2.3. Способи безпосереднього вчинення шахрайства у сфері використання інтернет-банкінгу	**100**
	1) фішинг	
	2) спамінг	
	3) кардинг	
	2.4. Способи приховування шахрайських дій у сфері використання інтернет-банкінгу	**100**
	1) знищення ЕОТ, яку використовували під час учинення шахрайських дій	**69**
	2) маскування вірусних програм під їх справжні аналоги	**32**
	3) відмова від надання показань	**58**

	4) використання VPN та інших засобів маскування місцезнаходження ЕОТ	**43**
	5) дача завідомо неправдивих показів (зокрема щодо неправдивого алібі) під час проведення процесуальних дій (допит, одночасний допит раніше допитаних осіб)	**31**
3	**Відомості про слідову картину протиправного діяння**	
	3.1 Матеріальні слід	**47**
	3.2. Цифрові сліди (віртуальні, електронні, комп'ютерні)	**100**
	а) профілях соціальних мереж (Facebook, Instagram, Twiter)	
	б) месенджерах (Telegram, Viber)	
	в) застосунках для переписок криптовалютного спрямування (Binance, OKX)	
	г) кеш-пам'яті онлайн магазинів	
	д) базах інтернет-провайдерів	
	3.3. Ідеальні сліди	**41**
5	**Особа потерпілого**	
	5.1. Віктимогенні групи потерпілих:	
	1) особи, які через вплив родичів та знайомих повідомили їм свої ідентифікатори доступу до інтернет-банкінгу	
	2) особи, які підлягли впливу незнайомих осіб та повідомили їм свої ідентифікатори доступу до інтернет-банкінгу	
	3) особи, які повідомили власні ідентифікатори доступу до інтернет-банкінгу працівникам банківської сфери	
6	**Дані про особу злочинця**	
	6.1. Стать:	
	1) чоловіча	**74**
	2) жіноча	**26**
	6.2. Вік:	
	1) від 16 до 20 років	**7**
	2) від 20 до 30 років	**34**
	3) від 30 до 40	**31**
	4) від 40 до 50	**20**
	5) особи віком 50 років і старше	**6**
	6.3. Освіта:	
	1) базова середня	**2**
	2) середня	**3**
	3) середня спеціальна	**5**
	4) базова вища	**27**
	5) вища	**63**
	6.4. Місце проживання:	
	1) не є місцевим жителем	**92**
	2) проживає на території вчиненого шахрайства	**8**
	6.5. Сімейний стан:	
	1) у шлюбі	**26**

	2) ні	**74**
	6.6. Шахрайські дії вчинялись у складі ОГ та ЗО:	
	1) так	**34**
	2) ні	**66**
	6.7. Склад ОГ та ЗО, яка здійснює шахрайські дії у сфері використання інтернет-банкінгу:	
	1) організатори	
	2) адміністратори сайтів, де розміщують неправдиві відомості про товари або надання послуг	
	3) продавці, які спілкуються з потенційними потерпілими (здебільшого через телефонні розмови або sms-переписки)	
	4) спамери (особи, які здійснюють розсилку листів стосовно інтернет-магазинів з продажу товарів або надання різноманітних послуг)	
	5) фішери (особи, які розсилають листи для отримання особистої інформації потенційних потерпілих)	
	6) програмісти (особи, які створюють спам-боти для розсилки та віруси для потенційних атак)	
	7) хакери (особи, які здійснюють вірусні атаки на об’єкти, що зацікавили злочинну організацію)	
	8) охоронці	
	9) корумповані представники органів державної влади й управління, працівники правоохоронних органів, які беруть участь у прикритті організованої злочинної діяльності	
	6.8. Рід занять:	
	1) учень (студент)	**15**
	2) працюючий	**55**
	– зокрема, у сфері фінансової діяльності та сфері комп’ютерних технологій	**91**
	6.9. Наявність судимості:	**5**
	6.10. Шахрайські дії вчинено у стані сп’яніння:	
	1) алкогольного	**1**
	2) наркотичного	**1**
	6.11. Особи, які шахрайські дії у сфері використання інтернет-банкінгу, відрізняються досить високим інтелектуальним рівнем:	
	1) так	**88**
	2) ні	**12**
	ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ	
7	Первинна інформація, що стала підставою для внесення відомостей в ЄРДР за фактом вчинення шахрайських дій була одержана уповноваженими особами з наступних джерел**:**	
	1) заяви, листи та повідомлення, що надійшли від потерпілих від шахрайських дій	**67**

	2) заяви, листи та повідомлення від громадян, які стали свідками вчинення шахрайських дій або одержали про них інформацію	**12**
	3) звернення, заяви, листи та повідомлення від співробітників фінансових установ різних форм власності	**9**
	4) матеріали справ, що було виокремлено з інших кримінальних проваджень	**5**
	5) матеріали, одержані при реалізації НСРД або розшукових заходів	**7**
8	**Типові слідчі ситуації розслідування шахрайства у сфері використання інтернет-банкінгу:**	
	1) вчинено шахрайські дії, наявна особистісна доказова база, злочинця (шахрая) встановлено	**27**
	2) здійснено шахрайські дії, є особистісна доказова база, злочинця (шахрая) не встановлено	**52**
	3) вчинено шахрайські дії, наявна особистісна та матеріальна доказова база, злочинця (шахрая) не встановлено	**16**
	4) вчинено шахрайські дії, повністю відсутня доказова база	**5**
	СЛІДЧІ (РОЗШУКОВІ) ДІЇ, НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ТА ІНШІ ПРОЦЕСУАЛЬНІ ДІЇ:	
9	**Які СРД, НСРД та процесуальні дії проводились:**	
	1) огляд місця події	**100**
	2) допит потерпілого	**100**
	3) огляд ЕОТ	**100**
	4) допит свідка	**100**
	5) тимчасовий доступ до речей і документів	**81**
	6) допит підозрюваного	**100**
	7) обшук	**78**
	8) призначення та проведення експертиз	**100**
	9) слідчий експеримент	**2**
	10) пред’явлення особи для впізнання	**5**
	а) за голосом	**8**
	б) в натурі	**6**
	в) по фото	**86**
	11) одночасний допит раніше допитаних осіб	**66**
	12) огляд документів	**27**
10	**Огляд:**	
	9.1. Проводився:	
	1) робоче місце потерпілого	
	2) робоче місце підозрюваного	
	3) банкомати	
	4) місця доступу до загальної мережі Wi-Fi	
11	**Обшук:**	
	10.1. Місця, де проводились:	

	1) місця зберігання та обробки даних про використання інтернет-банкінгу (сервери відповідних банківських установ, ЕОТ шахраїв)	**65**
	2) місця знаходження ЕОТ, яку використовували для вчинення шахрайських дій,	**43**
	3) місця зберігання відомостей, отриманих злочинним шляхом,	**38**
12	**Які НСРД проводились найчастіше:**	
	1) візуальне спостереження за особою	
	2) негласне зняття інформації з транспортних телекомунікаційних мереж	
13	**Допит:**	
	13.1. Ситуації за конфліктністю:	
	1) безконфліктні	**21**
	1) конфліктні	**79**
14	**Одночасний допит:**	
	14.1. Між ким проводився:	
	1) між підозрюваним та потерпілим	**87**
	2) між підозрюваним та свідками	**2**
	3) між підозрюваними особами	**9**
	4) між потерпілими	**1**
	5) між потерпілим та свідком	
	14.2. Результат одночасного допиту:	
	1) підозрюваний повністю або частково засвідчив свідчення, які раніше заперечував	**71**
	2) підозрюваний знову заперечував свідчення	**29**
15	**Залучення спеціаліста до процесуальних дій:**	
	1) огляд місця події	**100**
	2) огляд ЕОТ	**100**
	3) тимчасовий доступ до речей та документів	**62**
	4) обшук	**65**
	5) допит	**14**
	6) одночасний допит раніше допитаних осіб	**9**
	7) аудіоконтроль особи шляхом встановлення технічних засобів у публічно недоступному місці	**100**
	6) зняття інформації з транспортних телекомунікаційних мереж та електронних систем	**100**
16	**Експертизи:**	
	1) судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів, експертиза цифрової інформації, програмно-комп'ютерна експертиза)	
	2) судово-бухгалтерська експертиза	
	3) інформаційно-комп'ютерна експертиза	
	4) експертиза телекомунікаційних систем і засобів	

Додаток В

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.
2. Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.
3. Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).
4. Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.
5. Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.
6. Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234. (публікація тез)
8. Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200. (публікація тез)
9. Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової*

системи України : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123. (публікація тез)

10. Перхун С. О. До питання визначення обставин, які підлягають встановленню під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення* : матеріали Міжнар. наук.-практ. конф. (Київ, 13–14 берез. 2023 р.). Київ : Наук.-дослід. ін-т публіч. права, 2023. С. 131–133. (публікація тез)

Додаток Г

Акти впровадження результатів дисертаційного дослідження

ЗАТВЕРДЖУЮ
Перший проректор
Національної академії
внутрішніх справ
доктор юридичних наук, професор
полковник поліції

Станіслав ГУСАРЄВ

_____2024

АКТ

19. 04. 2024 м. Київ № 32

Впровадження результатів дисертації Перхуна Сергія Олександровича «Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі: т.в.о. начальника навчально-методичного відділу НАВС, лейтенанта поліції **В.О. Бойчук**, начальника відділу організації наукової діяльності та захисту прав інтелектуальної власності, підполковника поліції **В.В. Корольчука,** т.в.о. начальника відділу докторантури та ад'юнктури **А.П. Містюка,** т.в.о. завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, капітана поліції **Б.Ю. Бистрицького,** завідувача загальної бібліотеки **Л.Г. Гайдар**.

Комісія розглянула й узагальнила результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права **Перхуна Сергія Олександровича** на тему: **«Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу»** на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова

експертиза; оперативно-розшукова діяльність.

Проаналізовано основні результати дослідження С.О. Перхуна, зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

2. Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

3. Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).

4. Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

5. Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

6. Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

7. Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

8. Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200.

На основі проведеного аналізу комісія зробила висновок, що праці **С.О. Перхуна** містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Національної академії внутрішніх справ, зокрема при викладанні навчальних дисциплін «Криміналістика», «Криміналістичне забезпечення досудового розслідування», «Інновації у криміналістиці» та ін., під час підготовки навчально-методичних і дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

Вікторія БОЙЧУК

Віктор КОРОЛЬЧУК

Андрій МІСТЮК

Богдан БИСТРИЦЬКИЙ

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор
полковник поліції
Сергій ЧЕРНЯВСЬКИЙ
27.05 2024

АКТ

27.05 2024 м. Київ № 14

Впровадження результатів дисертації Перхуна Сергія Олександровича «Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі: начальника відділу організації наукової діяльності та захисту прав інтелектуальної власності, підполковника поліції **В.В. Корольчука,** т.в.о. начальника відділу докторантури та ад'юнктури **А.П. Містюка,** т.в.о. завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, капітана поліції **Б.Ю. Бистрицького,** завідувача загальної бібліотеки **Л.Г. Гайдар**.

Комісія розглянула й узагальнила результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права **Перхуна Сергія Олександровича** на тему: **«Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу»** на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Проаналізовано основні результати дослідження С.О. Перхуна, зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).

Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200.

Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової системи України* : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123.

На основі проведеного аналізу комісія зробила висновок, що праці **С.О. Перхуна** містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в науковій діяльності Національної академії внутрішніх справ, зокрема через проведення подальших наукових досліджень з проблем криміналістики, підготовку наукових робіт, видання монографії за результатами наукової роботи.

Члени комісії:

Віктор КОРОЛЬЧУК

Андрій МІСТЮК

Богдан БИСТРИЦЬКИЙ

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор
Дніпровського державного
університету внутрішніх справ
доктор юридичних наук, професор,
Заслужений діяч науки і техніки України
полковник поліції

Олександр ЮНІН

«__» _____ 2024 року

АКТ
впровадження у наукову діяльність
Дніпровського державного університету внутрішніх справ
результатів дисертаційного дослідження

Про впровадження у наукову діяльність Дніпровського державного університету внутрішніх справ результатів дисертаційного дослідження Перхуна С.О. «Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу» 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 комісії: т.в.о. начальника відділу організації наукової роботи Дніпровського державного університету внутрішніх справ, кандидата історичних наук, доцента Прошина Д.В.

члени комісії: заступника директора ННІ права та підготовки фахівців для підрозділів Національної поліції Дніпровського державного університету внутрішніх справ, доктора юридичних наук, доцента, полковника поліції Обшалова С.В.

професора кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ, доктора юридичних наук, професора Пирога І.В.

професора кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ, доктора юридичних наук, професора Єфімова М.М.

відповідно до Пріоритетних напрямів наукових досліджень Дніпровського державного університету внутрішніх справ на 2023-2024 навчальний рік склала

цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Перхуна С.О. на тему: «Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. Основні результати дослідження використовуються у НДіДКР Дніпровського державного університету внутрішніх справ для подальшої розробки проблемних питань методики розслідування кримінальних правопорушень проти власності та відображено у наукових публікаціях здобувача (статтях і тезах доповідей на конференціях):

Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).

Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : НДІПП, 2021. С. 198–200.

Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової системи України* : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123.

На основі проведеного аналізу комісія зробила висновок, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, відповідність спеціальності 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» та планам Науково-дослідних та дослідно-конструкторських робіт ДДУВС на 2023-2024 н.р., а також були враховані профільними кафедрами Дніпровського державного університету внутрішніх справ при проведенні науково-практичних заходів з актуальних питань застосування кримінального процесуального законодавства, проблем протидії протиправним діям проти власності та методики розслідування окремих видів кримінальних правопорушень, а також наукових досліджень на замовлення Головного Управління Національної поліції в Дніпропетровській області.

Голова комісії: **Денис ПРОШИН**

Члени комісії: **Сергій ОБШАЛОВ**

Ігор ПИРІГ

Микола ЄФІМОВ

ЗАТВЕРДЖУЮ
Начальник УСР
в Дніпропетровській області
ДСР НП України
полковник поліції
Віктор ЛЛДЕНКО
«07» 06 2024 року

АКТ
впровадження у практичну діяльність УСР в Дніпропетровській області ДСР НП України результатів дисертаційного дослідження Перхуна Сергія Олександровича «Теоретичні та практичні основи методики розслідування шахрайства у сфері використання інтернет-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала комісія у складі:

голови: начальник 9-го відділу (моніторингу та координації) УСР в Дніпропетровській області ДСР НП України, підполковник поліції, кандидат юридичних наук А.В. Макашов

члени комісії:
начальник 8-го відділу (інформаційно-аналітичного забезпечення) УСР в Дніпропетровській області ДСР НП України, майор поліції Д.С. Приходько
старший оперуповноважений 4-го відділу (протидії ОЗГ в органах державної влади) УСР в Дніпропетровській області ДСР НП України майор поліції П.А. Петраш
старший оперуповноважений 5-го відділу (боротьби з ОЗГ з ознаками корупції) УРВ в Дніпропетровській області ДСР НП України майор поліції Д.М. Мирошниченко

Комісія відповідно до Положення про організацію проведення науково-дослідних та дослідно-конструкторських робіт у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15 травня 2007 року № 154 склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження Перхуна Сергія Олександровича «Теоретичні та практичні основи методики розслідування шахрайства у сфері використання інтернет-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за

спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у вигляді наукових статей і тез доповідей на науково-практичних конференціях та семінарах, зокрема:

1. Перхун С. О. Особливості подальшого етапу розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2020. № 12. С. 145–150.

2. Перхун С. О. Початковий етап розслідування шахрайства у сфері використання інтернет-банкінгу: теоретичні та практичні аспекти. *Держава та регіони*. Серія: Право. 2021. № 4 (74). С. 234–238.

3. Перхун С. О. Типові слідчі ситуації під час розслідування шахрайства у сфері використання інтернет-банкінгу: наукові дискусії. *Knowledge, Education, Law, Management*. 2022. № 7 (51). С. 339–342. (Республіка Польща).

4. Перхун С. О. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Юридичний науковий електронний журнал*. 2023. № 6. С. 805–807.

5. Перхун С. О. Наукова полеміка щодо формування методики розслідування шахрайства у сфері використання інтернет-банкінгу. *Правові новели*. 2023. № 21. Т. 2. С. 164–171.

6. Перхун С. О. Актуальні питання побудови алгоритмів дій уповноважених осіб під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 145–149.

7. Перхун С. О. Наукові дискусії стосовно побудови структури криміналістичної характеристики шахрайства у сфері використання інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнар. наук.-практ. конф. (Київ, 12–13 серп. 2020 р.). Київ : Наук.-дослід. ін-т публіч. права, 2020. С. 232–234.

8. Перхун С. О. Криміналістична характеристика організованих груп і злочинних організацій, що вчиняють шахрайства у сфері використання інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнар. наук.-практ. конф. (Київ, 22–23 верес. 2021 р.). Київ : Наук.-дослід. ін-т публіч. права, 2021. С. 198–200.

9. Перхун С. О. Окремі аспекти використання спеціальних знань під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Проблемні питання юридичної науки в контексті реформування правової системи України* : матеріали Міжнар. наук.-практ. конф. (Київ, 19–20 жовт. 2022 р.). Київ : Наук.-дослід. ін-т публіч. права, 2022. С. 121–123.

10. Перхун С. О. До питання визначення обставин, які підлягають встановленню під час розслідування шахрайства у сфері використання інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення* : матеріали Міжнар. наук.-практ. конф. (Київ, 13–14 берез. 2023 р.). Київ : Наук.-дослід. ін-т публіч. права, 2023. С. 131–133.

Комісія вважає, що представлені матеріали дисертаційного дослідження, фахові наукові статті та тези доповідей, отримані на основі

проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також можуть бути впроваджені у діяльність управління стратегічних розслідувань в Дніпропетровській області ДСР НП України.

Голова комісії: **Антон МАКАШОВ**

Члени комісії: **Данило ПРИХОДЬКО**

Павло ПЕТРАШ

Дмитро МИРОШНИЧЕНКО

ЗАТВЕРДЖУЮ
Заступник начальника Головного слідчого управління Національної поліції України – начальник управління організації роботи та методичного забезпечення, доктор юридичних наук, професор, заслужений юрист України
полковник поліції

Артем ШЕВЧИШЕН

16 лютого 2024 року

АКТ № 141233-2024

Про впровадження у практичну діяльність Головного слідчого управління Національної поліції України результатів дисертаційного дослідження

Уклала комісія у складі:

Голови: начальника відділу методичної роботи та правового забезпечення Головного слідчого управління Національної поліції України, кандидата юридичних наук, полковника поліції Владислава Бурлаки

членів комісії: начальника сектору аналітичної роботи Головного слідчого управління Національної поліції України, кандидата юридичних наук, полковника поліції Олександра Волкова

старшого слідчого в особливо важливих справах відділу методичної роботи та правового забезпечення Головного слідчого управління Національної поліції України, майор поліції Аліни Віткалової

комісія відповідно до доручення Національної поліції України № 34684/24/4/3-2022 від 20.12.2022 «Про впорядкування процедури видання актів впровадження наукових досліджень у діяльність органів досудового розслідування Національної поліції України», склала цей акт, щодо розгляду основних положень та результатів дисертаційного дослідження Перхуна Сергія Олександровича на тему: «Теоретичні та практичні основи формування методики розслідування шахрайства у сфері використання інтернет-банкінгу»,

поданого на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 081 (Право).

Комісією встановлено, що висновки, які містяться в дисертаційному дослідженні, можуть використовуватись у практичній діяльності слідчих підрозділів Національної поліції України під час проведення занять в системі службової підготовки, а також при проведенні семінарів, нарад, а викладені у них пропозиції та рекомендації можуть бути корисними під час розслідування шахрайства у сфері використання інтернет-банкінгу.

Матеріали викладені у висновках до дисертаційного дослідження можуть використовуватись під час підготовки листів-роз'яснень до органів досудового розслідування Національної поліції України, оскільки мають як необхідний теоретичний та методологічний рівень, так і практичну цінність, що сприятиме вдосконаленню їх процесуальної діяльності.

Голова комісії: **Владислав БУРЛАКА**

Члени комісії: **Олександр ВОЛКОВ**

Аліна ВІТКАЛОВА