НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису
УДК 343.98: 343.131

СИСОЛЯТІН ВАЛЕРІЙ ВІКТОРОВИЧ

ДИСЕРТАЦІЯ

РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ

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

Подається на здобуття наукового ступеня кандидата юридичних наук
(доктора філософії)

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

В.В. Сисолятін

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

Київ – 2024

АНОТАЦІЯ

Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук (доктора філософії) за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність (081 – Право). – Науково-дослідний інститут публічного права; Дніпропетровський державний університет внутрішніх справ, Київ, 2024.

У дисертації на монографічному рівні досліджено наукові та практичні основи методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь, зокрема: а) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері власності; б) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері господарської діяльності; в) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку.

Сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в якій виокремлено наступні елементи: 1) криміналістична класифікація протиправних діянь; 2) криміналістична характеристика кримінальних правопорушень; 3) аналіз початкової інформації щодо вчиненого діяння; 4) обставини, що підлягають встановленню; 5) типові слідчі ситуації та відповідний їм алгоритм дій уповноважених осіб; 6) профілактична діяльність уповноважених осіб зі встановлення причин й умов, що сприяли учиненню кримінальних правопорушень; 7) взаємодія підрозділів правоохоронних органів та інших структур у кримінальному провадженні;

8) початковий етап досудового розслідування; 9) подальший етап досудового розслідування; 10) особливості використання спеціальних знань.

Удосконалено теоретичні концепції стосовно інформативного наповнення криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, яка складається з таких елементів: спосіб і обстановка вчинення кримінального правопорушення, слідова картина, особа злочинця та особа потерпілого.

Сформовано систему способів безпосереднього вчинення досліджуваної категорії кримінальних правопорушень: 1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг); 2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 4) розповсюдження шкідливих програмних чи технічних засобів або їхній збут з використанням мережі Інтернет; 5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах; 6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін.

Встановлено сукупність відомостей відносно обстановки вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, з урахуванням нормативно-правових, просторово-часових, соціальних, психологічних та економічних чинників.

Встановлено перелік можливих місць учинення кримінальних правопорушень: місця розташування електронно-обчислювальної техніки, з якої вчинювалися протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 61 %; місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %; місце знаходження потерпілого, який виявив факт учинення кримінальних правопорушень,

пов’язаних із використанням інтернет-банкінгу – 12 %.

Акцентовано увагу на системі відомостей стосовно віртуальних (електронних, комп’ютерних) слідів, що визначають слідову картину протиправного діяння та їхню взаємозалежність діям правопорушника з підготовки, вчинення й приховування кримінального правопорушення та обстановкою, у якій вони утворилися.

Сформовано сукупність криміналістичних ознак та властивостей особи правопорушника, на основі яких утворено його ймовірний «портрет» злочинця.

Надано криміналістичні ознаки й властивості осіб, які є потерпілими від кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, завдяки виокремленню відповідних віктимогенних груп.

Запропоновано пропозиції з приводу аналізу початкової інформації та на їх основі прийняття обґрунтованого висновку щодо початку досудового розслідування.

Окреслено коло обставин, що підлягають встановленню: 1) обставини, що характеризують вчинення кримінальних правопорушень, пов’язаних з використанням інтернет-банкінгу: а) відомості про час, місце та спосіб учинення протиправних дій, як-от, застосовування шкідливих програм чи вірусів, заведених до комп’ютерного забезпечення потерпілого та дублювання за допомогою них акаунту на власний ґаджет (смартфон, планшет, ноутбук, комп’ютер); б) відомості про віртуальні сліди кримінального правопорушення; в) встановлення місця одержання безпідставного доступу до мережі Інтернет; д) засоби, які застосовувалися під час скоєння протиправного діяння (технічні – різні ґаджети, зокрема, смартфони, ноутбуки, модеми; програмні – шпигунські програми, браузери, шкідливі віруси); 2) обставини, які розкривають особу правопорушника з різних сторін (професійної, злочинної. розумової); 3) обставини, які розкривають особу потерпілого з різних сторін (професійної, злочинної. розумової); 4) причинно-наслідкові взаємозв’язки: факт чіткого зв’язку між

діями правопорушників та їх наслідками; 5) обставини, які обтяжують чи пом'якшують покарання, або у цілому виключають кримінальну відповідальність за скоєння протиправних діянь, пов'язаних із використанням інтернет-банкінгу.

Сформульовано положення відносно планування та організації розслідування досліджуваної категорії протиправних діянь.

Запропоновано систему запобіжних заходів, котрі необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні досліджуваної категорії протиправних діянь, зокрема: 1) застосовування протоколів безпеки, зокрема, використання криптографічних функцій, а також системи аутентифікації користувачів шляхом перевірки правильності внесених даних і запобігання заміни особи; 2) застосовування технологій фіксації транзакцій, для прикладу, блокчейн, що допускають фіксувати всю інформацію; 3) повідомлення громадян через ЗМІ, соціальні мережі та месенджери (Viber, Telegram, WhatsApp) про факти скоєння кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу (фішинг, кардинг); 4) встановлення осіб, які схильні до антисуспільної поведінки в інформаційній сфері та постановка їх на відповідні обліки у підрозділах правоохоронних органів (зокрема, кіберполіції).

Надано перелік тактичних завдань, які повинні вирішуватись працівниками правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також розроблено комплекси дій для їх вирішення в рамках реалізації початкового та подальшого етапів розслідування.

Запропоновано систему типових слідчих ситуацій під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, зокрема: 1) скоєно кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, має місце достатня доказова база, особу правопорушника встановлено – 6 %; 2) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника не

встановлено – 64 %; 3) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника встановлено, та протиправні дії приховані під легальну фінансову діяльність – 9 %; 4) скоєно протиправне діяння, має місце заява потерпілого, відсутня будь-яка доказова база – 21 %.

Визначено сукупність криміналістичних версій, які можна висувати на початковому етапі розслідування: 1) кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, вчинене з метою отримання матеріальної вигоди «хакером»; 2) протиправне діяння вчинене з метою отримання матеріальної вигоди співробітником певної установи, яка володіє навичками роботи з комп'ютерною технікою; 3) протиправне діяння вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що має вільний доступ до визначеної комп'ютерної техніки; 4) протиправне діяння вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що не має вільного доступу до визначеної комп'ютерної техніки; 5) протиправне діяння вчинено з метою порушення алгоритму обробки даних, знищення або пошкодження комп'ютерних програм і баз даних, а так само їхніх носіїв.

Визначено принципи інформаційного забезпечення проведення слідчих (розшукових) дій початкового та подальшого етапів розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в розрізі інформаційного забезпечення допиту підозрюваних, свідків та потерпілих.

Розкрито організаційно-підготовчі заходи і тактику обшуку. Окреслено перелік об'єктів, які необхідно вилучати під час обшуку: 1) електронно-обчислювальна техніка, за допомогою якої здійснювалось втручання у роботу інтернет-мереж для їх дестабілізації або отримання відомостей, необхідних для реалізації операцій в інтернет-банкінгу (комп'ютери, планшети, ноутбуки, смартфони); 2) реквізити карток, що викрадені з серверів магазинів електронної торгівлі, платіжних і розрахункових систем, з персональних ґаджетів користувачів; 3) фотографії,

відеозаписи, на яких наявні дані, що мають значення для кримінального провадження; 4) квитанції про здійснення банківських операцій; 5) смартфони або інші ґаджети, в яких наявна адресна книга (ПІБ й адреси клієнтів фінансових установ, підприємств та організацій різних форм власності); 6) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб тощо.

Зосереджено увагу на допиті потерпілого та окреслено основні його завдання: з'ясувати обставини вчинення протиправного діяння (час, місце, зокрема, з доступом до загальної мережі Wi-Fi, наявність поблизу сторонніх осіб – можливість віддаленого підключення з іншого ґаджету); проаналізувати його передумови (чи були надіслані на номер потерпілого та прийняті повідомлення – в якому месенджері та якого змісту, чи були наявні дзвінки – в якому месенджері та якого змісту); встановити послідовність дій потерпілого після вчинення кримінального правопорушення (одразу повідомив в правоохоронні органи чи своїм знайомим, родичам, що зробив з ґаджетом – вимкнув, перезавантажив, продовжив користуватися). Визначено, що під час допиту потерпілого або свідка доцільно демонструвати певні об'єкти: а) скріншоти повідомлень переписки зі злочинцем; б) зображення (скріншот) документу, який підтверджує зняття коштів з рахунку потерпілого; в) виписку з банківського рахунку потерпілого; г) у випадках розмови зі злочинцем в телефонному режимі чи в режимі відео-конференції з'ясувати у потерпілого чи зробив він її запис – якщо так, то долучити до кримінального провадження для подальшого використання під час проведення пред'явлення для впізнання.

Визначено безконфліктні й конфліктні ситуації допиту підозрюваного. З'ясовано, що для вирішення конфліктних ситуацій застосовуються різноманітні тактичні прийоми допиту. Найбільш ефективним серед них вказано пред'явлення речових доказів, серед яких можуть демонструватись наступні об'єкти: свідчення потерпілих; протоколи пред'явлення для впізнання з позитивним результатом (підозрюваного впізнано за голосом чи в

натурі); флеш-накопичувачі та жорсткі диски з інформацією про банківські операції з грошовими коштами; скріншоти хмарних сховищ; скріншоти переписки з потерпілими.

Надано пропозиції відносно застосовування спеціальних знань у формі залучення спеціалістів відповідного профілю при їх безпосередній участі у процесуальних діях, зокрема: огляду комп'ютерної техніки – спеціаліст в галузі комп'ютерних технологій для ефективного виявлення та вилучення слідів правопорушення; допиту потерпілого – спеціаліста-фоноскопіста для роботи з голосовими даними (запис розмови потерпілого та правопорушника), які є в матеріалах кримінального провадження, а також подальшого призначення та проведення відповідних експертиз; обшуку – спеціаліст в галузі комп'ютерних технологій для ефективного вилучення електронно-обчислювальної техніки та носіїв інформації шляхом якісного подолання систем захисту, роботи з пристроями електроживлення, а також правильного зняття цифрових даних.

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

– *науковій діяльності* – під час реалізації наукових досліджень, спрямованих на розробку й удосконалення основ методики розслідування окремих видів кримінальних правопорушень у сфері власності й господарської діяльності, а також у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (акти впровадження Харківського національного університету внутрішніх справ від 06.04.2023 р., Національної академії внутрішніх справ від 23.05.2023 р.);

– *освітньому процесі* – при викладанні навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Тактичні особливості проведення слідчих (розшукових) дій», «Оперативно-розшукова діяльність»,

а також підготовці підручників, навчальних посібників, проведення практичних занять з кримінального процесу та криміналістики (акти впровадження ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» від 25.05.2023 р.);

– *законотворчій діяльності* – для покращення нормативно-правового забезпечення профілактики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, зокрема, в результаті наукового дослідження викладено низку пропозицій стосовно внесення змін і доповнень до діючих Кримінального процесуального кодексу України та Кримінального кодексу України;

– *правозастосовній діяльності* – для вдосконалення діяльності органів прокуратури, досудового розслідування, оперативних та експертних підрозділів Національної поліції (акти впровадження Дніпропетровського НДЕКЦ МВС від 19.05.2023 р.).

Ключові слова: *інтернет-банкінг, криміналістична характеристика, досудове розслідування, банківські операції, криміналістична класифікація, шахрайство, кіберзлочини, електронні перекази, кримінальне правопорушення, слідчі (розшукові) дії, спеціальні знання.*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані
основні наукові результати дисертації:

1. Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

2. 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).

3. 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. 127–132.

4. Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

5. 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.

6. 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.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

8. Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на*

сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

9. Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

10. 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.

SUMMARY

Sysoliatin V. V. Investigation of criminal offenses related with the using of Internet banking. – *Qualifying scientific work on manuscript rights.*

The thesis is for candidate's degree of law on specialty 12.00.09 – Criminal Procedure and Criminalistics; Forensic Examination; Operational-Search Activity. – Scientific Institute of Public Law; Dnipropetrovsk State University of Internal Affairs, Kyiv, 2024.

The dissertation at the monographic level examines the scientific and practical foundations of the methodology of investigating criminal offenses related to the use of Internet banking. A criminological classification of a certain category of illegal acts is proposed, in particular: a) criminal offenses related to the use of Internet banking in the sphere of property; b) criminal offenses related to the use of Internet banking in the field of economic activity; c) criminal offenses related to

the use of Internet banking, in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks.

The structure of a separate interspecies method of criminal offenses related to the use of Internet banking has been formed, in which the following elements are distinguished: 1) forensic classification of illegal acts; 2) forensic characteristics of criminal offenses; 3) analysis of initial information regarding the committed act; 4) circumstances to be established; 5) typical investigative situations and the corresponding algorithm of actions of authorized persons; 6) preventive activities of authorized persons to establish the causes and conditions that contributed to the commission of criminal offenses; 7) interaction of law enforcement units and other structures in criminal proceedings; 8) the initial stage of the pre-trial investigation; 9) further stage of pre-trial investigation; 10) features of using special knowledge.

The theoretical concepts regarding the informative content of the forensic characteristics of criminal offenses related to the use of Internet banking, which consists of the following elements: the method and circumstances of the commission of the criminal offense, the trail picture, the identity of the criminal and the identity of the victim, have been improved.

A system of methods of direct commission of the examined category of criminal offenses was formed: 1) fraudulent actions during the use of Internet banking (phishing, carding); 2) unauthorized interference in the operation of information (automated), electronic communication, information and communication systems, electronic communication networks; 3) illegal actions with transfer documents, payment cards and other means of access to bank accounts, electronic money, equipment for their production; 4) distribution of malicious software or technical means or their sale using the Internet; 5) unauthorized actions with information processed in computers; 6) intentional mass distribution of telecommunication messages, carried out without the prior consent of the addressees, which led to disruption or termination of computers, etc.

A collection of information regarding the circumstances of the commission of criminal offenses related to the use of Internet banking was established, taking into account regulatory, legal, spatial-temporal, social, psychological and economic factors.

A list of possible places where criminal offenses were committed was established: locations of electronic computing equipment used to commit illegal actions (stationary computer equipment, laptop, tablet, phone) – 61 %; locations of ATMs, institutions, enterprises and organizations of the financial sphere – 21 %; the location of the victim who discovered the fact of committing criminal offenses related to the use of Internet banking – 12 %.

Attention is focused on the system of information regarding virtual (electronic, computer) traces, which determine the trace pattern of an illegal act and their interdependence with the actions of the offender to prepare, commit and conceal a criminal offense and the environment in which they were formed.

A set of forensic signs and attributes of the offender's personality was formed, on the basis of which his probable «portrait» of the criminal was formed.

Forensic features and properties of persons who are victims of criminal offenses related to the use of Internet banking are provided, thanks to the identification of the relevant victimogenic groups.

Proposals are offered regarding the analysis of initial information and, based on them, the adoption of a reasoned conclusion regarding the initiation of a pre-trial investigation.

The circle of circumstances to be established is outlined: 1) circumstances characterizing the commission of criminal offenses related to the use of Internet banking: a) information about the time, place and method of committing illegal actions, such as the use of malicious programs or viruses introduced into the computer support of the victim and duplicating an account using them on your own gadget (smartphone, tablet, laptop, computer); b) information about virtual traces of a criminal offense; c) establishment of the place of obtaining unwarranted access to the Internet; d) means used during the commission of an illegal act (technical –

various gadgets, in particular, smartphones, laptops, modems; software – spyware, browsers, malicious viruses); 2) circumstances that reveal the identity of the offender from different angles (professional, criminal, mental); 3) circumstances that reveal the identity of the victim from different angles (professional, criminal, mental); 4) cause-and-effect relationships: the fact of a clear connection between the actions of offenders and their consequences; 5) circumstances that aggravate or mitigate punishment, or generally exclude criminal liability for committing illegal acts related to the use of Internet banking.

Provisions regarding the planning and organization of the investigation of the investigated category of illegal acts have been formulated.

A system of precautionary measures is proposed that must be implemented by authorized persons of law enforcement agencies when investigating the studied category of illegal acts, in particular: 1) application of security protocols, in particular, the use of cryptographic functions, as well as user authentication systems by checking the correctness of entered data and preventing identity substitution; 2) application of transaction recording technologies, for example, blockchain, which allow recording all information; 3) notification of citizens through mass media, social networks and messengers (Viber, Telegram, WhatsApp) about the facts of criminal offenses related to the use of Internet banking (phishing, carding); 4) identification of persons who are prone to anti-social behavior in the information sphere and putting them on the relevant records in law enforcement units (in particular, cyber police).

A list of tactical tasks that must be solved by law enforcement officers in criminal proceedings of the studied category is provided, as well as sets of actions for their solution in the framework of the implementation of the initial and subsequent stages of the investigation have been developed. A system of typical investigative situations during the investigation of criminal offenses related to the use of Internet banking is proposed, in particular: 1) a criminal offense related to the use of Internet banking has been committed, there is a sufficient evidence base, the identity of the offender has been established – 6 %; 2) an illegal act has been

committed, there is a sufficient evidence base, the identity of the offender has not been established – 64 %; 3) an illegal act has been committed, there is a sufficient evidence base, the identity of the offender has been established, and illegal acts are hidden under legal financial activity – 9 %; 4) an illegal act has been committed, the victim has made a statement, there is no evidence base – 21 %.

A set of forensic versions that can be put forward at the initial stage of the investigation is determined: 1) a criminal offense related to the use of Internet banking, committed with the aim of obtaining material benefit by a «hacker»; 2) the illegal act was committed for the purpose of obtaining material benefit by an employee of a certain institution who has computer skills; 3) the illegal act was committed with the purpose of acquiring information with limited access by a person (persons) who has free access to certain computer equipment; 4) the illegal act was committed with the purpose of acquiring information with limited access by a person (persons) who does not have free access to certain computer equipment; 5) the illegal act was committed with the aim of violating the data processing algorithm, destroying or damaging computer programs and databases, as well as their carriers.

The principles of information support for conducting investigative (search) actions of the initial and subsequent stages of the investigation of criminal offenses related to the use of Internet banking, in the context of information support for questioning suspects, witnesses and victims, have been determined.

The organizational and preparatory measures and tactics of the search were disclosed. The list of objects that must be removed during the search is outlined: 1) electronic computing equipment, which was used to intervene in the work of Internet networks to destabilize them or obtain information necessary for the implementation of operations in Internet banking (computers, tablets, laptops, smartphones); 2) details of cards stolen from servers of e-commerce stores, payment and settlement systems, from personal gadgets of users; 3) photographs, video recordings, which contain data relevant to criminal proceedings; 4) receipts for bank transactions; 5) smartphones or other gadgets in which there is an address

book (names and addresses of clients of financial institutions, enterprises and organizations of various forms of ownership); 6) notebooks, journals, handwritten texts with available data on the identity of the victim or other interested persons, etc.

Attention is focused on the interrogation of the victim and its main tasks are outlined: to find out the circumstances of the commission of the illegal act (time, place, in particular, with access to a public Wi-Fi network, the presence of outsiders nearby – the possibility of remote connection from another gadget); analyze its prerequisites (whether messages were sent to the victim's number and received – in which messenger and with what content, were there calls – in which messenger and with what content); to establish the sequence of the victim's actions after committing a criminal offense (immediately reported to the law enforcement agencies or his friends and relatives what he did with the gadget – turned it off, rebooted, continued to use it).

It was determined that during the interrogation of a victim or a witness, it is advisable to show certain objects: a) screenshots of messages of correspondence with the criminal; b) an image (screenshot) of a document confirming the withdrawal of funds from the victim's account; c) a statement from the victim's bank account; d) in the case of a conversation with a criminal by phone or video conference, find out from the victim whether he made a recording of it – if so, then attach it to the criminal proceedings for further use during the presentation for identification.

Non-conflict and conflict situations of interrogation of the suspect are defined. It was found that various tactical methods of interrogation are used to resolve conflict situations. The most effective among them is the presentation of physical evidence, among which the following objects can be demonstrated: testimony of the victims; reports of presentation for identification with a positive result (the suspect was identified by voice or in kind); flash drives and hard drives with information on bank transactions with cash; screenshots of cloud storage; screenshots of correspondence with victims.

Proposals were made regarding the application of special knowledge in the form of involving specialists of the appropriate profile during their direct participation in procedural actions, in particular: review of computer equipment – a specialist in the field of computer technology for effective identification and removal of traces of a crime; interrogation of the victim – a phonoscopist specialist for working with voice data (recording of the conversation between the victim and the offender), which is in the materials of the criminal proceedings, as well as the further appointment and conduct of relevant examinations; search – a specialist in the field of computer technologies for the effective extraction of electronic computing equipment and data carriers by qualitatively overcoming protection systems, working with power supply devices, as well as correctly removing digital data.

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:

– *scientific activity* – during the implementation of scientific research aimed at the development and improvement of the foundations of the methodology of investigation of certain types of criminal offenses in the sphere of property and economic activity, as well as in the sphere of the use of electronic computing machines (computers), systems and computer networks and telecommunications networks (implementation acts of the Kharkiv National University of Internal Affairs dated 04/06/2023, of the National Academy of Internal Affairs dated 05/23/2023);

– *the educational process* – when teaching the educational disciplines «Organization of the investigation of criminal offenses», «Criminal studies», «Criminal process», «Tactical features of conducting investigative (search) actions», «Operational and investigative activities», as well as the preparation of textbooks, training manuals, conducting practical classes on criminal procedure and criminology (acts of implementation of PrJSC «Higher educational institution «Interregional Academy of Personnel Management» dated May 25, 2023);

– *law-making activity* – to improve the regulatory and legal support for the prevention of criminal offenses related to the use of Internet banking, in particular, as a result of a scientific study, a number of proposals regarding the introduction of changes and additions to the current Criminal Procedure Code of Ukraine and the Criminal Code of Ukraine were laid out;

– *law enforcement activities* – to improve the activities of the prosecutor's office, pre-trial investigation, operational and expert units of the National Police (acts of implementation of the Dnipropetrovsk NDEKC of the Ministry of Internal Affairs dated May 19, 2023).

Keywords: *Internet banking, forensic characteristics, pre-trial investigation, banking operations, forensic classification, fraud, cybercrimes, electronic transfers, criminal offense, investigative (search) actions, special knowledge.*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані
основні наукові результати дисертації:

1. Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

2. 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).

3. 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. 127–132.

4. Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

5. 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.

6. 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.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

8. Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

9. Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му*

сторіччі : матеріали Міжнародної науково-практичної конференції (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

10. 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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ГУНП – Головне управління Національної поліції

ЕОМ – Електронно-обчислювальна машина

ЕОТ – Електронно-обчислювальна техніка

ЕПС – Електронні платіжні системи

ЄРДР – Єдиний реєстр досудових розслідувань

ІКЕ – Інформаційно-комп’ютерна експертиза

КК – Кримінальний кодекс

КМЕ – Комп’ютерно-мережева експертиза;

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

НСРД– Негласна слідча (розшукова) дія

ОГ – Організовані групи

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

ЦК – Цивільний кодекс України

ЦПК – Цивільний процесуальний кодекс України

п. – Пункт

р. – Рік

с. – Сторінка (сторінки)

ст. – Стаття

ч. – Частина

ВСТУП

Обґрунтування вибору теми дослідження. Світ невпинно розвивається, здійснюються нові наукові відкриття, дедалі запроваджуються процеси діджиталізації суспільства, створюються сучасні цифрові технології. Такі новації ефективно використовуються в економічній сфері, у секторі державного управління, суспільстві та приватному житті. Формуються новітні поняття – криптовалюта, інтернет-банкінг, е-бізнес, «Qiwi-гаманець», MoneyGram, Perfect Money, е-комерція, blockchain) та ін. Цифрові процеси значно змінюють архітектоніку фінансових, комерційних та сервісних операцій, що позитивно впливає на розвиток суспільства. Останнім часом більшість провідних компаній перейшли на діджиталізований формат співпраці, що дозволяє швидко здійснювати комерційні операції, укладати угоди та перераховувати гроші. Безумовно, такими новаціями не могли не скористуватися представники кримінальних угрупувань (хакери, фішери), які дедалі частіше роблять спроби швидко заволодіти коштами як пересічних громадян, так і підприємств, установ та організацій різних форм власності. Наразі перед правоохоронними органами, насамперед, підрозділами Національної поліції, постають нагальні питання створення діючих алгоритмів встановлення вказаних осіб, попередження їх неправомірних посягань та ефективного розслідування протиправних діянь.

За даними узагальнення правоохоронної практики встановлено, що серед вказаних кримінальних правопорушень є великий масив тих, що пов’язані з використанням інтернет-банкінгу.

Отже, відповідно до відомостей Офісу Генерального прокурора України до ЄРДР за 2018 рік було внесено 3366 фактів шахрайств, учинених з використанням високих інформаційних технологій, а обвинувальний акт було вручено лише у 847 випадках. У тому ж році за іншими статтями КК України, що пов’язані з використанням інтернет-банкінгу, була майже подібна ситуація або навіть гірша: ст. 200 КК – 609 випадків обліковано, 505 обвинувальних

актів; ст. 222 КК – 58 випадків обліковано, 27 обвинувальних актів; ст. 231 КК – 272 випадків обліковано, 103 обвинувальних акта; ст. 232 КК – 11 випадків обліковано, а обвинувальні акти взагалі відсутні; ст. 361 КК – 1023 випадків обліковано, 479 обвинувальних актів; ст. 361^1 КК – 134 випадки обліковано, 79 обвинувальних актів; ст. 361^2 КК – 52 випадки обліковано, 23 обвинувальних актів; ст. 362 КК – 1070 випадків обліковано, 740 обвинувальних актів; ст. 363^1 КК – 10 випадків обліковано, 8 обвинувальних актів. Протягом наступних років статистика майже не змінювалася. Для підтвердження, наведемо статистичні дані за перші 5 місяців 2023 року: ст. 200 КК – 185 випадків обліковано, 103 обвинувальних акта; ст. 222 КК – 8 випадків обліковано та лише 1 обвинувальний акт; ст. 231 КК та ст. 232 КК відповідно 1 та 4 випадки обліковано, а обвинувальні акти взагалі відсутні; ст. 361 КК – 810 випадків обліковано, 356 обвинувальних актів; ст. 361^1 КК – 21 випадків обліковано, 3 обвинувальних акта; ст. 361^2 КК – 45 випадків обліковано, 7 обвинувальних актів; ст. 362 КК – 853 випадків обліковано, 406 обвинувальних актів; ст. 363^1 КК – 3 випадки обліковано, а обвинувальні акти взагалі відсутні. Наведені показники вказують на те, що кількість кримінальних правопорушень визначеної категорії щороку дедалі збільшується, а кількість правопорушників, за якими складено обвинувальний акт, – залишається на досить незначному рівні. Окрім того, більшість протиправних дій мають високий рівень латентності, внаслідок чого значна кількість фактів залишаються невикритими.

Низька якість розслідування кримінальних проваджень і незначна кількість викритих та притягнутих до відповідальності злочинців зумовлені низкою чинників: відсутність чіткої взаємодії й належної координації окремих підрозділів Національної поліції (зокрема, співробітників кіберполіції та слідчих) – 71 %, невчасне здійснення СРД, НСРД та інших процесуальних заходів – 61 %, поверхневе використання техніко-криміналістичних засобів під час проведення окремих процесуальних дій та ігнорування залучення відповідних спеціалістів – 79 %, відсутність

міжнародної практики розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу – 82 %, порушення послідовності дій під час збирання доказів на початковому етапі кримінального провадження – 62 %, невизначеність заходів щодо профілактики злочинних проявів – 91 % та ін.

Теоретичне підґрунтя дисертаційного дослідження становлять ґрунтовні праці, написані науковцями з різних напрямків юридичної науки (криміналістики, кримінального процесу, кримінології, кримінального права, оперативно-розшукової діяльності), що є вагомим внеском у методику розслідування окремих видів кримінальних правопорушень. Це визнані правознавці та дослідники, а саме: Ю. П. Аленін, І. В. Басиста, В. П. Бахін, В. Д. Берназ, В. К. Весельський, А. Ф. Волобуєв, В. Г. Дрозд, М. М. Єфімов, В. А. Журавель, А. В. Іщенко, Н. І. Клименко, В. О. Коновалова, В. С. Кузьмічов, В. В. Лисенко, В. Г. Лукашевич, Є. Д. Лук’янчиков, В. Л. Ортинський, І. В. Пиріг, М. В. Салтевський, Р. Л. Степанюк, В. Є. Тарасенко, В. В. Тіщенко, П. В. Цимбал, К. О. Чаплинський, С. С. Чернявський, Ю. М. Чорноус, В. Ю. Шепітько та ін.

Проблемні питання кримінально-процесуального, криміналістичного та оперативно-розшукового забезпечення розслідування кіберзлочинів, кримінальних правопорушень у сфері використання банківських електронних платежів або учинених через мережу Інтернет висвітлювалися у наукових працях: А. І. Анапольської, О. В. Герасимова, Б. М. Головкіна, І. А. Гукової, О. І. Деньковича, О. В. Добрової, О. Ю. Довженка, А. Е. Жиліна, Т. В. Коршикової, В. Б. Коби, І. О. Коваленка, О. В. Курмана, В. В. Луцика, О. І. Мотляха, В. Р. Мойсика, О. Л. Мусієнко, Т. В. Охрімчук, Н. В. Павлової, В. І. Пазиніч, Д. А. Птушкіна, А. В. Рейнгольда, А. В. Реуцького, Д. О. Рички, О. А. Самойленко, С. В. Самойлова, Т. Л. Тропіної, В. Г. Хахановського, Д. М. Цехана, К. О. Чередник, С. С. Чернявського, С. В. Чучка та ін.

Серед сучасних наукових розробок можна виділити дисертацію О. Ю. Довженка «Основи методики розслідування кіберзлочинів» (м. Харків,

2020 р.), у якій автор визначив стан наукової розробки проблем розслідування кіберзлочинів, встановив основні підходи до класифікації кіберзлочинів і запропонував на їх основі інтегрований підхід; надав криміналістичну характеристику кіберзлочинів як особливого типу злочинів, розглянув особливості допиту потерпілих, свідків, підозрюваних і обвинувачуваних у справах про кіберзлочини, виявив особливості отримування доказів і проведення експертиз у справах про кіберзлочини. У свою чергу, С. В. Чучко у дисертації «Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет» (м. Дніпро, 2021 р.) охарактеризував особливості правового регулювання правовідносин у віртуальному просторі, що впливають на рівень вчинення шахрайства у мережі Інтернет, здійснив науковий аналіз обстановки вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет та особливості їх слідової картини, сформулював систему типових слідчих ситуацій початкового етапу розслідування та висвітлив особливості використання спеціальних знань під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет. Наразі колектив авторів у складі Б. М. Головкіна, О. І. Деньковича, В. В. Луцика і Д. М. Цехана у навчальному посібнику «Кіберзлочинність та електронні докази» (м. Львів, 2022 р.) визначив види кіберзлочинів, поняття кіберзлочинності та її місце у загальній структурі злочинності, окреслив особливості методики розслідування кіберзлочинів, охарактеризував електронні докази у кримінальному провадженні. А. Е. Жилін у дисертації «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів» (м. Дніпро, 2023 р.) розкрив стан наукових досліджень питань протидії шахрайствам у сфері використання банківських електронних платежів, охарактеризував основні елементи криміналістичної характеристики досліджуваного виду шахрайства, розглянув взаємодію слідчих та оперативних підрозділів Національної поліції, сформулював заходи профілактичної діяльності працівників правоохоронних органів щодо виявлення й усунення причин та умов

шахрайства у сфері використання банківських електронних платежів, виокремив тактичні операції стосовно збирання початкових відомостей про обставини події та виявлення ознак шахрайства, визначив перелік заходів під час проведення тактичної операції «Електронно-обчислювальна техніка».

Проте, незважаючи на теоретичну значущість наведених праць, більшість вчених обмежилися дослідженням лише проблемних аспектів розслідування кіберзлочинів або окремих видів шахрайств чи інших суміжних протиправних діянь. На сьогодні відсутнє комплексне дослідження міжвидової методики розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, особливо в умовах запровадженого воєнного стану. Наведені обставини у своїй сукупності визначили актуальність окресленої проблематики, її теоретичне й практичне значення, а також зумовили вибір напряму дисертаційної роботи.

Зв’язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до положень Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації (розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р), Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020), Стратегії воєнної безпеки України (Указ Президента України від 25.03.2021 № 121/2021), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 03.03.2021 № 179), Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р), Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р), Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки (Указ Президента України від 11.05.2023

№ 273/2023), Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України (спільний наказ Офісу Генерального прокурора та МВС України від 22.11.2021 № 371/846), тематики наукових досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022-2026 роки (наказ МОН України від 03.02.2022 № 109), тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11.06.2020 № 454), Основних напрямів наукових досліджень Науково-дослідного інституту публічного права на 2020–2024 рр.

Мета і задачі дослідження. *Мета* дисертаційного дослідження виявляється у розв'язанні конкретного наукового завдання з розробки теоретичних засад методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

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

– узагальнити наукові погляди стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та запропонувати їхню криміналістичну класифікацію;

– визначити сучасні наукові підходи до розуміння криміналістичної характеристики як складової методики розслідування протиправних діянь досліджуваної категорії;

– охарактеризувати окремі елементи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу;

– здійснити криміналістичний аналіз первісної інформації та сформулювати коло обставин, що підлягають встановленню у кримінальному провадженні;

– конкретизувати типові слідчі ситуації, що виникають на початковому етапі розслідування, а також відповідні кожній з них алгоритми дій працівників правоохоронних органів;

– визначити особливості початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу;

– охарактеризувати подальший етап розслідування у кримінальних провадженнях досліджуваної категорії;

– виокремити особливості використання спеціальних знань під час розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу.

Об’єктом дослідження є кримінальні процесуальні відносини, що виникають у діяльності правоохоронних органів під час розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу.

Предмет дослідження – розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу.

Методи дослідження. У дисертації використано різні методи наукового пізнання, спираючись на визначені мету, завдання, об’єкт і предмет дослідження. Основним є діалектичний метод, що визначає вагомість взаємодії складових будь-якої системи та їх взаємозв’язок для її ефективної діяльності. Зокрема, *порівняльно-правовий метод* використовувався при **опрацюванні** кримінально-процесуальних і кримінальних норм, **системи процесуальних дій, а також деяких** нормативно-правових актів (розділи 1–3). Застосовування *методу формальної логіки* надало змогу детально з’ясувати сутність криміналістичної характеристики кримінального правопорушення та виокремити її основні складові (підрозділи 1.1-1.2). Використання *історико-правового методу* зумовлено необхідністю опрацювання ґенези наукових поглядів щодо кримінальних правопорушень досліджуваної категорії (підрозділ 1.1). *Системно-структурний метод* дозволив здійснити криміналістичну класифікацію правопорушень, пов’язаних із використанням інтернет-банкінгу, а також класифікацію типових способів їх підготовки, безпосереднього учинення й приховування;

виділення віктимогенних груп потерпілих (розділ 1). *Метод моделювання* застосовувався під час формулювання загальних висновків та конкретних пропозицій стосовно вдосконалення КК та КПК України (розділи 1–3). *Документальний, соціологічний* та *статистичний методи* використано під час узагальнення результатів опитування респондентів та аналізу матеріалів кримінальних проваджень (розділи 1–3), а також під час з'ясування недоліків організаційно-тактичного забезпечення проведення окремих процесуальних дій під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу (розділи 2–3). *Типологічний метод* – **використано для створення** «портрету» ймовірного правопорушника та виокремлення віктимогенних груп потерпілих **(підрозділ 1.3).** На основі *синтезу* сформульовано загальні висновки за темою дослідження (розділи 1–3).

Емпіричну основу дослідження становлять **згруповані відомості Єдиного звіту про вчинені кримінальні правопорушення Офісу Генерального прокурора України та** Департаменту інформаційно-аналітичної підтримки Національної поліції **за період 2018-2023 рр., а також** результати узагальнення оперативної, слідчої та судової практики протягом 2015-2023 рр. Зокрема, опрацьовано матеріали 247 кримінальних проваджень за напрямом дослідження (Волинська, Дніпропетровська, Донецька, Закарпатська, Запорізька, Івано-Франківська, Київська, Кіровоградська, Львівська, Миколаївська, Одеська, Сумська, Ужгородська, Харківська та Чернівецька області, м. Київ), а також проаналізовано зведені результати опитувань 151 працівника прокуратури, 316 слідчих, 376 працівників оперативних підрозділів та 84 працівників експертних установ МВС України. Під час дослідження використано власний досвід роботи в правоохоронних органах України.

Наукова новизна одержаних результатів полягає у тому, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням основ методики розслідування кримінальних

правопорушень, пов’язаних із використанням інтернет-банкінгу, в якому сформульовано низку наукових положень і практичних рекомендацій, **спрямованих на підвищення ефективності діяльності органів досудового розслідування Національної поліції України,** що вирізняються науковою новизною та мають важливе теоретичне і практичне значення, зокрема:

уперше:

– запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь, зокрема: а) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у сфері власності; б) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у господарській діяльності; в) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у питанні використання електронно-обчислювальних машин (комп’ютерів), систем і комп’ютерних мереж та мереж електрозв’язку;

– сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, в якій виокремлено такі елементи: 1) криміналістична класифікація протиправних діянь; 2) криміналістична характеристика; 3) аналіз початкової інформації щодо вчиненого діяння; 4) обставини, що підлягають встановленню; 5) типові слідчі ситуації та відповідний їм алгоритм дій уповноважених осіб; 6) профілактична діяльність уповноважених осіб зі встановлення причин й умов, що сприяли учиненню кримінальних правопорушень; 7) взаємодія підрозділів правоохоронних органів та інших структур у кримінальному провадженні; 8) початковий етап розслідування; 9) подальший етап розслідування; 10) особливості використання спеціальних знань;

– запропоновано систему запобіжних заходів, котрі необхідно здійснювати уповноваженим особам правоохоронних органів під час розслідування досліджуваної категорії протиправних діянь, зокрема: 1) застосовування протоколів безпеки, зокрема, використання криптографічних функцій, а також системи аутентифікації користувачів

шляхом перевірки правильності внесених даних і запобігання заміни особи; 2) застосовування технологій фіксації транзакцій, для прикладу, блокчейн, що допускають фіксувати всю інформацію; 3) повідомлення громадян через ЗМІ, соціальні мережі та месенджери (Viber, Telegram, WhatsApp) стосовно фактів скоєння кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу (фішинг, кардинг); 4) встановлення осіб, які мають нахили до антисуспільної поведінки в інформаційній сфері та постановка їх на відповідні обліки у підрозділах правоохоронних органів (зокрема, кіберполіції);

– надано перелік тактичних завдань, що мають вирішуватись працівниками правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також розроблено комплекси дій для їх вирішення в рамках реалізації початкового та подальшого етапів розслідування;

удосконалено:

– теоретичні концепції стосовно інформативного наповнення криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу;

– систему таких способів безпосереднього вчинення досліджуваної категорії кримінальних правопорушень: 1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг); 2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 4) розповсюдження шкідливих програмних чи технічних засобів або їхній збут з використанням мережі Інтернет; 5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах; 6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін.;

– сукупність відомостей відносно обстановки вчинення кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, з урахуванням нормативно-правових, просторово-часових, соціальних, психологічних та економічних чинників;

– перелік можливих місць учинення кримінальних правопорушень: місця розташування електронно-обчислювальної техніки, з якої вчинювалися протиправні дії (стаціонарне комп’ютерне обладнання, ноутбук, планшет, телефон) – 61 %; місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %; місце знаходження потерпілого, який виявив факт учинення кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу – 12 %;

– криміналістичні ознаки та властивості осіб, які є потерпілими від кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, завдяки виокремленню відповідних віктимогенних груп;

– пропозиції з приводу аналізу початкової інформації та на їх основі прийняття обґрунтованого висновку щодо початку досудового розслідування;

– систему обставин, що підлягають встановленню у кримінальному провадженні;

– сукупність криміналістичних версій, які можна висувати на початковому етапі розслідування: 1) кримінальне правопорушення, пов’язане з використанням інтернет-банкінгу, вчинене з метою отримання матеріальної вигоди «хакером»; 2) протиправне діяння вчинене з метою отримання матеріальної вигоди співробітником певної установи, який володіє навичками роботи з комп’ютерною технікою; 3) протиправне діяння вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що має вільний доступ до визначеної комп’ютерної техніки; 4) протиправне діяння вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що не має вільного доступу до визначеної комп’ютерної техніки; 5) протиправне діяння вчинено з метою порушення алгоритму обробки даних, знищення або пошкодження комп’ютерних програм і баз даних, а так

само їх носіїв;

– принципи інформаційного забезпечення проведення слідчих (розшукових) дій початкового та подальшого етапів розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, в розрізі інформаційного забезпечення допиту підозрюваних, свідків та потерпілих;

Набули подальшого розвитку:

– наукові положення щодо напрямів теоретичних досліджень із проблем розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу, враховуючи умови запровадженого воєнного стану;

– система відомостей стосовно віртуальних (електронних, комп’ютерних) слідів, що визначають слідову картину протиправного діяння та їх взаємозалежність діям правопорушника з підготовки, вчинення й приховування кримінального правопорушення та обстановкою, у якій вони утворилися;

– сукупність криміналістичних ознак і властивостей особи правопорушника, на основі яких утворено його ймовірний «портрет» злочинця;

– положення відносно планування та організації розслідування досліджуваної категорії протиправних діянь;

– система типових слідчих ситуацій під час розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу;

– організація і тактика проведення слідчих (розшукових) дій для вилучення інформації з матеріальних та особистісних джерел з урахуванням завдань, що потребують вирішення під час їх підготовки та проведення, а також проведення окремих негласних слідчих (розшукових) дій, серед яких варто виділити наступні: спостереження за об’єктом, прослуховування телефонних переговорів, зняття інформації з транспортних та електронних

систем;

– пропозиції відносно застосовування спеціальних знань у формі залучення спеціалістів відповідного профілю за умови їх безпосередньої участі у процесуальних діях, зокрема: огляду комп'ютерної техніки – спеціаліст у галузі комп'ютерних технологій для ефективного виявлення та вилучення слідів правопорушення; допиту потерпілого – спеціаліста-фоноскопіста для роботи з голосовими даними (запис розмови потерпілого та правопорушника), що є в матеріалах кримінального провадження, а також подальшого призначення та проведення відповідних експертиз; обшуку – спеціаліст у галузі комп'ютерних технологій для ефективного вилучення електронно-обчислювальної техніки та носіїв інформації шляхом якісного подолання систем захисту, роботи з пристроями електроживлення, а також правильного зняття цифрових даних.

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

– *науковій діяльності* – під час реалізації наукових досліджень, спрямованих на розробку й удосконалення основ методики розслідування окремих видів кримінальних правопорушень у сфері власності й господарської діяльності, а також у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку (акти впровадження Харківського національного університету внутрішніх справ від 06.04.2023, Національної академії внутрішніх справ від 23.05.2023);

– *освітньому процесі* – під час викладання навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Тактичні особливості проведення слідчих (розшукових) дій», «Оперативно-розшукова діяльність», а також підготовки підручників, навчальних посібників, проведення практичних занять із кримінального процесу та криміналістики (акти

впровадження ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» від 25.05.2023);

– *законотворчій діяльності* – для покращення нормативно-правового забезпечення профілактики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, зокрема, в результаті наукового дослідження викладено низку пропозицій стосовно внесення змін і доповнень до діючих Кримінального процесуального кодексу України та Кримінального кодексу України;

– *правозастосовній діяльності* – для вдосконалення діяльності органів прокуратури, досудового розслідування, оперативних та експертних підрозділів Національної поліції (акти впровадження Дніпропетровського НДЕКЦ МВС від 19.05.2023).

Апробація результатів дисертації. Основні теоретичні положення й висновки дисертації оприлюднено на міжнародних науково-практичних конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 2020 р.), «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 2021 р.), «Перспективні напрямки розвитку юридичної науки у 21-му сторіччі» (м. Київ, 2022 р.), «Пріоритетні напрями розвитку юридичної науки в умовах сьогодення » (м. Київ, 2023 р.).

Публікації. Основні положення та результати дисертації відображено у десяти наукових публікаціях, із яких п'ять статей – у виданнях, включених МОН України до переліку наукових фахових видань із юридичних наук, одна – у закордонному юридичному виданні, чотири – у збірниках тез наукових доповідей, оприлюднених на 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 230 сторінок, з яких 158 сторінок основного тексту. Список використаних

джерел налічує 191 найменування та займає 22 сторінки, 4 додатки викладено на 27-и сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ

1.1. Ґенеза наукових поглядів стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та їх криміналістична класифікація

Кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу, з кожним роком збільшуються як в своїй кількості, так і в якості. Адже розвиток комп'ютерних технологій та мережі Інтернет не зупиняється ні на мить. Тому й правопорушники, які вчиняють досліджувані протиправні діяння, застосовують все новіші засоби та способи їх скоєння. В той же час, працівники правоохоронних органів повинні не відставати від вказаної категорії осіб, а навпаки – намагатися їх випереджати та передбачати їх наступні кроки. В свою чергу, це вимагає від науковців здійснювати сучасні дослідження з практичними рекомендаціями для попередження та розслідування визначених протиправних діянь [138, с. 457].

Слід акцентувати увагу на «цифровізації» суспільства. А також зазначити, що на сьогодні термін «цифровізація» вживають у значно широкому розумінні, у тому числі і як «цифрову революцію» в економіці, суспільстві та приватному житті. З приводу історії виникнення кіберзлочинності в цілому звернемося до різних джерел та їх опрацюємо. Зокрема, окрема група дослідників надає інформацію, що в 1971 році було створено перший у світі комп'ютерний вірус «Кріпер», який після проникнення в систему залишав повідомлення: «Я – Повзун. Спіймай мене якщо зможеш». Також автори вказують, що в 1982 році учень середньої школи Річард Скрент «…розробив вірус Elk Cloner, перший вірус, який

заразив операційну систему Apple II… 1986 – Прийнято перший закон США про шахрайство та зловживання з використанням комп’ютерів (Computer Fraud and Abuse Act, CFAA), основний нормативно-правовий акт, що встановлює кримінальну відповідальність за злочини у сфері комп’ютерної інформації, який в подальшому неодноразово доповнювався… 1990 рік – Великобританія ухвалила Закон про неправомірне використання комп’ютерів, який криміналізував несанкціоновані спроби доступу до IT-систем… 2013 рік – Американський рітейлер Мета – розкриття персональних даних 40 мільйонів клієнтів кредитних карток». Крім того, дослідники наголошують, що в 2020 році у зв’язку із загрозою вірусу COVID-19 багато компаній по всьому світу швидко перейшло до віддаленої роботи, внаслідок чого дуже сильно зросла небезпека вибуху корпоративних бізнес-мереж [107]. Як бачимо, починаючи ще з 70-их років XX-го сторіччя через розвиток електронно-обчислювальної техніки виникали як дуже позитивні моменти її використання, так і негативні фактори під час діяльності окремих осіб. Слід зазначити, що на протязі значного періоду протиправні діяння, що вчинялися за допомогою електронно-обчислювальної техніки, взагалі не характеризувались як кримінальне правопорушення.

Інша група авторів приводить в приклад наступну ситуацію: «У 2004 році в мережі одного з підприємств оборонного концерну Lockheed-Martin китайські хакери прорвали систему захисту комп'ютерів, залишили безліч слідів свого перебування у вигляді троянів та бекдорів. Досі не зрозуміло, чи хакери встигли скопіювати важливі дані, але частина даних компанії була сильно зіпсована. Не оминули хакери та комп'ютерну мережу американського Міністерства оборони, сисадміни якого навіть не помічали, що зловмисники ось уже 2 роки мають вільний доступ до цінної інформації. Уряд США звинуватив у хакерській атаці російських програмістів, але Офіційний Кремль це звинувачення спростував» [51].

А вже Г. В. Загіка акцентував увагу на тому, що навіть великі компанії (як Apple Computer) теж не захищені від нападу. Зокрема, автор приводить

наступну ситуацію: «В грудні 1987 р. ця фірма знайшла вірус у своїй системі електронної пошти. Цьому вірусу вдалося знищити всі мовні повідомлення та відключити систему». Також науковець зробив висновок, що напад на фінансові організації вчинюється у багатьох випадках її службовцями, які є професіоналами своєї справи. Зокрема, дослідник зауважив, що проведені у США опитування показують, що саме службовці, які мають знання в галузі комп'ютерної техніки, відіграють головну роль у вчиненні комп'ютерних протиправних діянь, адже без застосування криптографічних методів захисту інформації практично не можливо реально захистити інформацію. Г. В. Загіка вказує на те, що сучасна криптографія базується на новітніх досягненнях математики, фізики, інженерних дисциплін та у галузі розробки та використання комп'ютерних технологій. Як підсумок, автор вказує, що до правових норм слід віднести розробку та прийняття норм, які встановлюють відповідальність за порушення інтелектуальної власності, за комп'ютерні правопорушення [42, с. 57]. Тобто ще на початку 2000-их років (дата публікації статті – 2002 рік) різні науковці на території України почали досліджувати питання протидії кіберзлочинності.

В свою чергу, О. Л. Порфімович виокремив кілька основних завдань, виконання яких потребує комплексного підходу, як-от, систематичне збирання розвідувальних даних про потенційні кібертерористичні загрози та ресурси, а також забезпечення захисту життєво важливих елементів вітчизняної інфраструктури (передбачає окрему статтю фінансування органів державної влади та управління). Крім того, дослідник акцентував увагу на розробці технологій превенції комп'ютерних нападів (співпраця з науковими та науково-дослідними установами та організаціями) та на зведенні до мінімуму прогалин у вітчизняному законодавстві. Також автор вирізнив зниження рівня латентності комп'ютерних правопорушень та припинення масового використання в різних сферах не захищеного належним чином програмного забезпечення. Як висновок, дослідник вказав, що найкращим способом боротьби проти злочинності у галузі високих технологій є найвищі технології

та стимул науково-технічного прогресу, що має слугувати справі протидії кіберзлочинності [108]. Інакше кажучи, на часі одним із головних пріоритетів України повинно бути належне грошове забезпечення проєктів, які направлені на створення прогресивних технологій у сфері протидії кіберзлочинності.

Зі свого боку, О. Ю. Довженко констатував, що злочинна діяльність, так саме як і все людське життя, стають все більш «діджиталізованими». Також вказаний автор, як і О. Л. Порфімович, наголошував на тому, що за таких умов, розробка нових підходів до боротьби з кіберзлочинністю є однією з найбільш гострих завдань кримінально-правової та криміналістичної науки. Адже мова, на думку науковця, йде не просто про нову групу протиправних діянь, а про новий та такий, що швидко розвивається, тип протиправної поведінки – кіберзлочинність. Крім того, вчений-криміналіст акцентував увагу на особливій складності вказаної проблеми завдяки інтернаціоналізованому характеру злочинних посягань, вчинених за допомогою електронних пристроїв та мережі Інтернет. Як висновок, О. Ю. Довженко вказав, що ефективна боротьба з кіберзлочинністю силами лише однієї країни неможлива, тому потрібна спільна діяльність правоохоронних відомств усіх країн, з використанням єдиної методології розслідування кіберзлочинів, що забезпечувала б засудження кіберзлочинців незалежно від національних кордонів [24, с. 1]. Як бачимо, ще один вітчизняний дослідник наголосив на важливості активізації наукових досліджень в розрізі протидії та розслідування кіберзлочинів.

Окрема група авторів надала характеристику криміналістичних особливостей початкового етапу розслідування шахрайства з фінансовими ресурсами у кіберпросторі, його значення, аналіз та обґрунтування як одного з видів кіберзлочинності, що є небезпечним для кожного, а також довела необхідність реалізації невідкладних заходів щодо попередження та протидії визначених кримінальних правопорушень. Крім того, науковці зробили висновок, що ефективність протидії інтернет-шахрайству та рівень

кібербезпеки в Україні на дуже низькому рівні [186, с. 141-142]. Інша група вчених-криміналістів та процесуалістів наголосила на тому, професійне шахрайство є глобальною проблемою, хоча деякі результати відрізняються від країни до країни, але більшість тенденцій зберігається. Автори одним із ключових завдань правоохоронних органів визначили створення ефективної та стабільної системи підготовки фахівців, які володітимуть технологіями розслідування кримінальних правопорушень, пов'язаних з легалізацією (відмиванням) доходів, одержаних незаконним шляхом, зокрема, доходів, отриманих за допомогою шахрайських бухгалтерських схем [190, с. 166].

А вже В. Зарубей, О. Гумін та О. Римарчук акцентували увагу на тому, що зараз, в важкій економічній ситуації, в Україні набуло поширення шахрайство в різних сферах життя людини. Автори зазначили, що зростання кількості та якості таких протиправних діянь призводить до значних втрат фінансових ресурсів не лише громадян, а й держави в цілому. Тому актуальним питанням нашого сьогодення є дослідження механізму швидкого, повного та ефективного розслідування та попередження визначених кримінальних правопорушень. В Україні, на думку науковців, триває активне інформування населення про способи вчинення досліджуваної категорії протиправних діянь та створення заходів захисту конфіденційної інформації. Проте офіційна статистика свідчить про значний обсяг випадків вчинення шахрайства, а також про недостатній рівень його розкриття. Як висновок, однією з причин В. Зарубей, О. Гумін та О. Римарчук виокремлюють застарілі методи розслідування шахрайства та відсутність методів розслідування окремих його видів [191, с. 63]. Тобто усі вищеперераховані вітчизняні дослідники вказують на наявну проблематику опрацюванні різних видів кримінальних правопорушень, що входять в предмет нашого дослідження.

З приводу публікацій зарубіжних авторів, одразу приведемо як приклад В. Клея, який в своїй праці «Комп'ютерні атаки та кібертероризм: вразливі місця та політичні питання для Конгресу» (2005 р.) наголошував на

тому, що багато інтернаціональних терористичних груп використовують комп'ютери та Інтернет для координованих атак проти комп'ютерної системи США. Також дослідник надав характеристику різним видам атак (фізичній, електронній та кібератаці). Крім того, автор вказав, що хакери шукають уразливості в комп'ютерних системах і атакують їх надзвичайно швидко [181].

В свою чергу, Л. Шеллі зауважував ще в 2003 році, що на той час спостерігалось активне використання існуючих форм проведення таємних операцій засобами інформаційних технологій. Також автор зазначав, що сюди входить все більш широке використання шифрування, переказ грошей за допомогою комп'ютерної системи та зростання шахрайства в Інтернеті. Крім того, дослідник відмічав, що позаяк транснаціональні злочинні групи та терористи залучають найкращих спеціалістів з інформаційних технологій, то, відповідно, варто очікувати нових та інноваційних способів використання інформаційних технологій вказаними групами. Тому найбільше занепокоєння багатьох урядів і міжнародних фінансових систем викликає можливість серйозних вторгнень у критично важливі системи. Вказані вторгнення, на думку Л. Шеллі, можуть включати уведення вірусів, які знищували б критично важливі відомості, розміщення шкідливих веб-сайтів, які не можна зруйнувати, і навіть повне виведення з ладу критично важливих комп'ютерних систем. Ще на початку XX-го сторіччя автор констатував, що нинішня взаємозалежність світової економічної системи означає, що порушення в одному регіоні світу матиме хвилеві наслідки в інших регіонах [184]. Тому ми повністю підтримуємо висновок дослідника стосовно того, що необхідно здійснювати постійний моніторинг ринків акцій, облігацій і товарів фінансовими аналітиками в усьому світі. І саме в такому випадку вторгнення або порушення роботи комп'ютерних систем не залишиться непоміченим. Наразі для цього можливо впровадити у всі вказані системи технологію «blockchain».

В такому ж ракурсі про небезпеку кібертероризму писав в своїй

публікації Дж. Льюїс. Автор наголошував на тому, що кібератаки, мережева безпека та інформація створюють складні проблеми, які виходять у нові сфери національної безпеки та державної політики. Також дослідник зауважив, що всі питання, які стосуються кібертероризму та кібератак на критичну інфраструктуру викликають негативні наслідки для національної безпеки. Крім того, Дж. Льюїс сформулював кібертероризм як використання інструментів комп'ютерної мережі для вимкнення критично важливих національних інфраструктур (таких як енергетика, транспорт, державні операції) або для примусу чи залякування уряду чи цивільного населення. Як висновок автор вказав, що передумовою кібертероризму є те, що в міру того, як країни та критична інфраструктура стають все більш залежними від комп'ютерних мереж для їх роботи, створюються нові вразливі місця – «велика електронна ахіллесова п'ята» [183].

Зі свого боку, Д. Деннінг опрацьовуючи проблематику діяльності активістів та кібертерористів, які використовують Інтернет, зробила висновок, громадські активісти видаються найефективнішими з цих акторів мережевої війни, а кібертерористи на сьогоднішній день (2001 р.) не становлять великої реальної загрози, але це може змінитися, якщо вони отримають кращі інструменти, техніки та методи організації, і якщо кіберзахист не встигне за ними [182]. Як бачимо з сьогоднішньої ситуації – кіберзлочинці отримали найкращі засоби для вчинення своїх протиправних діянь, а кіберзахист за ними не завжди встигає. Тобто прогноз дослідниці виправдався з гіршої сторони.

На останок приведемо позицію Ф. Уільямса, який наголошував на тому, що колумбійські організації, які займаються торгівлею наркотиками, дотримуються стандартної ділової практики для диверсифікації ринку та продукції. Автор акцентував увагу, що злочинні організації та торговці наркотиками все частіше наймають фінансових спеціалістів для здійснення операцій з відмивання грошей, що додає додатковий рівень прикриття, використовуючи юридичних і фінансових експертів, які знають фінансові

операції та наявність надійних місць в офшорних фінансових юрисдикціях. З огляду на зазначене дослідник вказує, що організованій злочинності не потрібно розвивати технічну діяльність в Інтернеті, адже у них є можливість просто найняти тих із хакерського співтовариства, які мають відповідний досвід, забезпечуючи за допомогою поєднання винагород і загроз ефективне виконання поставлених завдань. Оскільки у віртуальному світі немає кордонів – це робить його дуже привабливим для злочинної діяльності. А сам Інтернет, на думку науковця, надає можливості для різного роду крадіжок з онлайн-банків, інтелектуальної власності, пропонує сучасні способи вчинення шахрайства і виявляє нові вразливості, пов’язані з комунікаціями та даними, які є привабливими мішенями для вимагання, що завжди було основним елементом мафіозних організацій. Підсумовуючи, Ф. Уільямс зауважує, що анонімність Інтернету робить його ідеальним каналом та інструментом для багатьох дій організованої злочинності [185]. Як бачимо, секретність є ключовою частиною стратегії організованої злочинності, в той час як Інтернет пропонує чудові можливості для її створення та збереження, наприклад, різними інтернет-кафе, різними маршрутизаціями мережі Інтернет тощо.

З приводу нормативно-правового забезпечення звернемось до опрацювання відповідних нормативно-правових актів. Зокрема, в Конвенції про кіберзлочинність, ратифікованої Україною 07.09.2005 року визначено, які правопорушення вчиняються за допомогою комп’ютерних систем. В зазначеному документі вказано наступні групи протиправних діянь: правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6)); правопорушення, пов’язані з комп’ютерами (підробка, пов’язана з комп’ютерам (ст. 7), шахрайство, пов’язане з комп’ютерами (ст. 8)); правопорушення, пов’язані зі змістом (правопорушення, пов’язані з дитячою порнографією (ст. 9));

правопорушення, пов’язані з порушенням авторських та суміжних прав (ст. 10) [61]. Як бачимо, ще на початку 2000-их років міжнародні законодавці розуміли необхідність визначити конкретні протиправні діяння, які можуть здійснюватись з використанням комп’ютерних систем.

Також у визначеній Конвенції передбачено, що сторонами вживаються:

– законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до внутрішнього законодавства за навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів (ст. 11);

– законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи (ст. 12);

– законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань (ст. 14);

– встановлення, імплементацію і застосування повноважень і процедур, передбачених цією частиною, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини (ст. 15) [61].

З огляду на зазначене, можна зробити висновок, що вказані заходи відображають максимально широкі повноваження кожної держави, яка ратифікувала зазначену конвенцію (в тому числі, й України).

Крім того, менше ніж через два роки було підписано Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи, ратифікований Україною 21.07.2006 року. В даному документі надано визначення расистського та ксенофобного матеріалу, а саме вказано, що це будь-який письмовий матеріал, будь-яке зображення чи будь-яке інше

представлення ідей або теорій, які захищають, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій (ст. 2) [27]. Тобто в Додатковому протоколі визначено нагальні на той час питання дискримінації осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання. Вказані аспекти є і зараз актуальними в Україні, адже на часі неодноразово виникають ситуації пов'язані з нетерпимістю осіб через національне або етнічне походження та віросповідання.

В Додатковому протоколі теж передбачено, що сторонами вживаються наступні заходи:

– законодавчих й інших заходів, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до расистського та ксенофобного матеріалу (ст. 3);

– законодавчих й інших заходів, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: погроза, зроблена через комп'ютерну систему, вчинення тяжкого злочину, визначеного в її національному законодавстві, проти (i) осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (i) групи осіб, яка відрізняється за будь-якою з цих характеристик (ст. 4);

– законодавчих й інших заходів, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: публічна образа через комп'ютерну систему (i) осіб з причини їх належності до групи, яка відрізняється за

ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (і) групи осіб, яка відрізняється за будь-якою з цих характеристик (ст. 5);

– законодавчих й інших заходів, які можуть бути необхідними для визнання таких дій кримінальними правопорушеннями у її національному законодавстві, у разі умисного вчинення без права на це: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства (ст. 6);

– законодавчих й інших заходів, які можуть бути необхідними для визнання кримінальними правопорушеннями у її національному законодавстві, у разі умисного вчинення без права на це, пособництва або підбурювання до вчинення будь-якого з правопорушень, визначених відповідно до цього Протоколу, з наміром вчинити такий злочин [27].

Аналіз Кримінального кодексу України [74] та ряду інших нормативно-правових актів дозволяє зробити висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імплементовані в правове поле нашої держави.

Зокрема, рішенням Ради національної безпеки і оборони України ще 2016 р. було схвалено проект Стратегії кібербезпеки України [114], відповідно до якої було прийнято ряд законодавчих та інших актів. Для прикладу, в тому ж році Указом президента України було створено Національний координаційний центр кібербезпеки, серед основних завдань якого було визначено наступні: «…здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; здійснення аналізу: стану кібербезпеки; стану кіберзахисту критично важливих об'єктів інфраструктури» та інші [112].

А вже в Законі України «Про основні засади забезпечення кібербезпеки України» надано ряд основоположних визначень: індикатори кіберзагроз;

інформація про інцидент кібербезпеки; інцидент кібербезпеки (кіберінцидент); кібератака; кібербезпека; кіберзагроза; кіберзахист; кіберзлочин (комп'ютерний злочин); кіберзлочинність; кібероборона; кіберпростір; кіберрозвідка; кібертероризм; кібершпигунство; критична інформаційна інфраструктура та інші. Також у вказаному законодавчому акті визначено відповідних суб'єктів, «…які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; 8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом». Крім того, у вказаному Законі зазначено основних суб'єктів національної системи кібербезпеки, а сааме: «…Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України» [113]. Як бачимо, на законодавчому рівні сформовано досить широке коло підрозділів, на які покладено обов'язок забезпечувати національну систему кібербезпеки.

Крім того, в ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» надано перелік визначень термінів, які використовуються для позначення окремих категорій досліджуваної тематики, як-от: «…виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або

юридичним особам, що не мають права доступу до неї»; «захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі»; «інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле»; «криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо»; «порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст» тощо [111].

Також і в ст. 3 Закону України «Про електронну комерцію» наведено ряд понять, що використовуються для позначення окремих категорій досліджуваної тематики, зокрема: «електронний підпис одноразовим ідентифікатором – дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору»; «інтернет-магазин – засіб для представлення або реалізації товару, роботи чи послуги шляхом вчинення електронного правочину»; «реалізація товару дистанційним способом – укладення електронного договору на підставі ознайомлення покупця з описом товару, наданим продавцем у порядку, визначеному цим Законом, шляхом забезпечення доступу до каталогів, проспектів, буклетів, фотографій тощо з використанням інформаційно-комунікаційних систем, телевізійним, поштовим, радіозв’язком або в інший спосіб, що виключає можливість безпосереднього ознайомлення покупця з товаром або із зразками товару під час укладення такого договору» [109].

Стосовно останніх нововведень приведемо нові правила посиленої кібербезпеки в Євросоюзі. Зокрема, прийнята нова директива з кібербезпеки NIS 2 із січня 2023 року запроваджує обов’язкові заходи інформаційної

безпеки та вимоги до звітності про інциденти інформаційної безпеки. Серед них слід вказати те, що за невиконання цих вимог багато компаній у певних секторах будуть піддаватися значним штрафам. Всі країни-члени ЄС повинні внести вказаний акт у своє національне законодавство, адже NIS 2 набула чинності 16 січня 2023 року та повністю замінить чинну Директиву про безпеку мереж та інформаційних систем 17 жовтня 2024 року. Адже вказана директива встановлює вимоги до організацій, що надають найважливіші послуги у сфері енергетики, логістики, фінансів, охорони здоров'я, комунальних служб, цифрової інфраструктури, промисловості, державного управління та досліджень [22]. На жаль, поки що Україна не входить до країн ЄС та не зобов'язана ратифікувати наведену Директиву.

Проте незважаючи на прийняті нормативно-правові акти кількість звернень за фактами вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, дедалі зростає, злочинна діяльність набуває все більш латентного та організованого характеру. Заходи щодо протидії злочинним проявам з урахуванням запровадженого воєнного стану не відповідають сучасним загрозам і потребують удосконалення.

З приводу класифікації кримінальних правопорушень, вкажемо, що зазначене питання викликає суперечності в колі вчених-криміналістів. Деякі з них досить різко відзиваються з приводу вказаного нововведення, інші навпаки його підтримують. Ми поділяємо позицію останніх, тому розглянемо можливість класифікації кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Для прикладу, Б. В. Щур зауважував, що спроби створити криміналістичні класифікації протиправних діянь за криміналістичними критеріями є схвальними та потребують подальших наукових досліджень. Також автор зазначав, що «…не можна обмежуватися у класифікаційних побудовах лише криміналістичними ознаками (критеріями), а необхідно виходити з кримінально-правової класифікації злочинів, яка у цьому сенсі, фактично є базовою. Прагматична роль криміналістичної класифікації

злочинів, на думку автора, полягає у тому, що вона є основою для вироблення цілеспрямованих наукових рекомендацій та розроблення окремих криміналістичних методик. При цьому криміналістична класифікація злочинів передбачає врахування криміналістично значущих ознак» [178, с. 16].

У свою чергу, М. М. Єфімов, на основі опрацювання наукових праць різних авторів та в результаті вивчення матеріалів кримінальних проваджень вважав «…за необхідне класифікувати криміналістичну характеристику правопорушень проти моральності. Зокрема, відповідно до сфери моральності визначено наступні групи: 1) речових та особистісних прав громадян (ст.ст. 297–300 КК України); 2) статевих стосунків (ст.ст. 301–303 КК України); 3) діяльності осіб, що не досягли повноліття (ч. 4 с. 301, ч. 3–4 ст. 302, ч. 3–4 ст. 303, ст. 304 КК України)» [33, с. 57]. На нашу думку, вказана класифікація також корелюється з відповідною групою протиправних діянь і може вважатися класифікацією кримінальних правопорушень.

Зі свого боку, інша група дослідників (Р. С. Довбаш, С. С. Чернявський) запропонували класифікацію протиправних діянь здійснювати завдяки поєднанню кримінально-правових ознак та криміналістичних критеріїв на базові, споріднені та супутні. Зокрема, науковці зауважили, що «…базові злочини становлять визначальний елемент механізму злочинної діяльності. До цієї групи слід зараховувати головні, найчисельніші з яких визначають домінуючу спрямованість протиправної діяльності особи або групи осіб та задовольняють злочинну мету. Споріднені (допоміжні) злочини, протиправні прояви яких є способом або необхідною умовою підготовки, вчинення та приховування базових злочинів або окремих епізодів, маскування слідів протиправної діяльності тощо. Супутні злочини – схожі за багатьма ознаками з базовими, але мають деякі кримінально-правові та криміналістичні відмінності» [164, с. 22–23].

А вже О. Ю. Довженко зазначав, що сфера кіберзлочинності далека від врегулювання засобами кримінального права. На думку автора, варто

пристосувати до класифікації протиправних діянь за чинним Кримінальним кодексом класифікацію кіберзлочинів. Зокрема, науковець в ній виокремив такі групи кримінальних правопорушень: «…1. Злочини проти конституційних прав і свобод людини і громадянина. До них можна віднести порушення права на особисте та сімейне життя, порушення таємниці листування, порушення авторських і суміжних прав, що скоюються за допомогою комп'ютерних технологій чи мережі Інтернет. 2. Злочини проти життя та здоров'я населення, зокрема використання мережі Інтернет для розповсюдження заборонених чи обмежених у обігу речовин, таких як наркотики, психотропні речовини, ліки. 3. Злочини проти честі та гідності особи. До них можна віднести використання комп'ютерних технологій та мережі Інтернет для розповсюдження відомостей, що порочать честь та гідність особи. 4. Злочини проти власності. До них можна віднести викрадення грошових коштів з банківських рахунків, шахрайство та інші корисливі злочини, що ставлять на меті заволодіти власністю іншої особи з використанням комп'ютерних технологій і мережі Інтернет. 5. Злочини в сфері комп'ютерної інформації, зокрема неправомірний доступ до інформації, а також створення та використання шкідливих комп'ютерних програм. 6. Злочини проти суспільної моралі (найбільш відомим прикладом є виготовлення, зберігання й поширення порнографії, в тому числі дитячої). 7. Злочини проти безпеки держави, в тому числі, проти державної таємниці, скоєні з використанням комп'ютерних технологій чи мережі Інтернет. 8. Злочини терористичного характеру, зокрема заклики до тероризму, фінансування тероризму та безпосередньо акти кібертероризму» [23, с. 22].

Доречною також вважаємо позицію В. Ю. Шепітька, який вказував, що у випадках взяття складу кримінального правопорушення за основу для групування криміналістичних класифікацій вказаних діянь, то може бути створена система останніх. Також автор зауважив, що у криміналістиці пропонуються класифікації протиправних діянь за такими групами: «…1. Класифікації злочинів, пов'язаних із суб'єктом злочину, що

вчиняються: одноособово і групою; вперше і повторно; особами, що знаходяться в особливих відносинах з безпосереднім предметом посягання, та такими, що не перебувають у таких відносинах; дорослими злочинцями і неповнолітніми; чоловіками і жінками (ця класифікація має обмежену сферу застосування і належить тільки до деяких «суто чоловічих» злочинів або злочинів, учинення яких більш властиво жінкам). 2. Класифікація злочинів, пов'язаних з об'єктом злочину: за особою потерпілого; за характером безпосереднього предмета посягання; за місцем розташування безпосереднього предмета посягання (за місцем вчинення злочину); за способами і засобами охорони безпосереднього предмета посягання. 3. Класифікації злочинів, пов'язаних з об'єктивною стороною злочину: за способом вчинення злочину; за способом приховування злочину, якщо він не входить як складова частина до способу вчинення злочину. 4. Класифікації злочинів, пов'язаних із суб'єктивною стороною злочину: вчинені із заздалегідь обдуманим умислом та з умислом, що раптово виник» [72, с. 273-274].

Наостанок, приведемо на розгляд твердження О. Ю. Довженка, який зазначив, що протиправні діяння, які вчиняються за допомогою комп'ютерних технологій та мережі «Інтернет», варто виокремити в окрему групу – кіберзлочини, тобто такі кримінальні правопорушення, що скоєні за допомогою цифрових технологій [26, с. 79].

На основі наведених позицій вважаємо за потрібне надати власну криміналістичну класифікацію визначеної категорії протиправних діянь, засновану на характерних ознаках: за способом та умовами їх вчинення. Адже нами було встановлено, що низці кримінальних правопорушень, які передбачені КК України та віднесені до різних його розділів, притаманна загальна характеристика – вчинення з використанням інтернет-банкінгу. На підставі цього, запропоновано наступну криміналістичну класифікацію, як-от: а) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері власності; б) кримінальні правопорушення,

пов’язані із використанням інтернет-банкінгу, у сфері господарської діяльності; в) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у сфері використання електронно-обчислювальних машин (комп’ютерів), систем і комп’ютерних мереж та мереж електрозв’язку.

Підсумовуючи, зазначимо, що було проаналізовано ряд позицій дослідників та нормативно-правових актів з приводу протиправних діянь визначеної категорії. Стосовно наданої криміналістичної класифікації також слід зазначити, що вона не є досконалою з точки зору криміналістики. Оскільки, класифікація виходить не стільки з характеристики діяння, скільки з необхідності кваліфікувати вказані діяння за кримінальним правом. В той же час, якраз ця класифікація допускає застосування існуючого термінологічного апарату як Кримінального кодексу, так і різноманітних нормативно-правових актів (міжнародних та вітчизняних).

1.2. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу

Починаючи розгляд криміналістичної характеристики необхідно згадати про розвиток такої наукової категорії як методика розслідування окремих видів кримінальних правопорушень. Дану категорію опрацьовували різні вчені-криміналісти, як-от, А. Ф. Волобуєв [18], І. І. Когутич [58], В. А. Коченєва [67], В. Малюга [88], М. В. Салтевський [124], Р. Л. Степанюк [148], А. П. Шеремет [177] та інші.

Стосовно визначення самого поняття методики розслідування окремих видів кримінальних правопорушень, то, для прикладу, О. М. Дуфенок формулював її як «…логічну побудову, складові якої повинні різнобічно забезпечувати уповноважену особу теоретичними знаннями щодо оптимального та ефективного ходу досудового розслідування». Крім того, автор зауважував, що у її структурі окремої криміналістичної методики варто

виділити наступні складові: «…1. Криміналістична характеристика злочину. 2. Особливості збирання, аналізу та оцінювання інформації на стадії внесення відомостей до ЄРДР. 3. Обставини, що підлягають установленню під час кримінального провадження. 4. Типові слідчі ситуації, що виникають під час розслідування злочину. 5. Типові слідчі версії та планування досудового розслідування злочину. 6. Типові слідчі дії на початковому, подальшому та завершальному етапах розслідування злочину. 7. Особливості застосування науково-технічних засобів і спеціальних знань. 8. Профілактична робота слідчого за матеріалами розслідування. 9. Взаємодія слідчих, оперативно-розшукових, експертних та інших підрозділів у практичній діяльності розслідування злочинів» [71, с. 506-507].

А вже група науковців (К. О. Чаплинський, О. В. Лускатов, І. В. Пиріг, В. М. Плетенець) виділяли в структурі окремої криміналістичної методики такі складові як-от: 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 [69, с. 346].

В свою чергу, інші вчені-криміналісти виокремлювали в системі визначеної наукової категорії такі складові: «…криміналістична характеристика даного виду злочинів; обставини, що підлягають доказуванню; типові слідчі ситуації, що виникають на різних етапах розслідування, слідчі версії та планування; особливості виявлення того чи іншого виду злочинів (внесення відомостей до Єдиного реєстру досудових розслідувань); початковий етап розслідування, тактика проведення першочергових слідчих (розшукових) дій гласного та негласного характеру; наступний етап розслідування, тактика проведення окремих слідчих (розшукових) дій на цьому етапі; особливості взаємодії слідчого з оперативними підрозділами; особливості використання слідчим спеціальних знань в процесі розслідування; заходи криміналістичної профілактики за

матеріалами розслідування» [85, с. 204].

Зі свого боку, В. Ю. Шепітько зазначав, що «при всьому різноманітті окремих методик у них є типові елементи, система яких утворює структуру окремих методик. До них можна віднести: 1) криміналістичну характеристику злочинів даного виду; 2) обставини, що підлягають з'ясуванню по справі; 3) особливості виявлення ознак того або іншого виду злочинів; 4) дії в стадії порушення кримінальної справи; 5) початковий етап розслідування; тактику першочергових слідчих дій і оперативно-розшукових заходів; 6) наступний етап розслідування; тактику наступних дій та інших заходів; 7) профілактичні дії слідчого» [72, с. 271].

Доцільною також вважаємо думку М. М. Єфімова, який в структурі методики розслідування окремих видів кримінальних правопорушень виділяв наступні елементи: «…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» [35, с. 14-15].

Підсумовуючи, слід зазначити, що на основі вищенаведених позицій нами було сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в якій виокремлено наступні елементи:

1) криміналістична класифікація протиправних діянь;

2) криміналістична характеристика;

3) аналіз початкової інформації щодо вчиненого діяння;

4) обставини, що підлягають встановленню;

5) типові слідчі ситуації та відповідний їм алгоритм дій уповноважених осіб;

6) профілактична діяльність уповноважених осіб зі встановлення причин й умов, що сприяли учиненню кримінальних правопорушень;

7) взаємодія підрозділів правоохоронних органів та інших структур у кримінальному провадженні;

8) початковий етап розслідування;

9) подальший етап розслідування;

10) особливості використання спеціальних знань.

Як бачимо, в наведених системах, як і у сформованій нами, майже завжди наявна така складова як криміналістична характеристика. Говорячи про криміналістичну характеристику правопорушень, пов'язаних з використанням інтернет-банкінгу, для початку необхідно визначитись з формулюванням її поняття. Зазначену категорію досліджувало багато науковців, зокрема, серед них необхідно виокремити таких як В. П. Бахін та Б. Є Лук'янчиков [7], В. О. Малярова [89], Р. Л. Степанюк [151] тощо.

Наприклад, В. В. Тіщенко говорив про те, що «…у розслідуванні нерозкритих кримінальних правопорушень корисливо-насильницької спрямованості криміналістичний аналіз встановлених обставин дозволяє виявити між ними спільні та особливі риси, зробити висновок про можливе скоєння цих протиправних діянь однією і тією ж особою або однією і тією ж групою осіб. Такий висновок може бути зроблений не лише на основі повної криміналістичної характеристики кожного окремого кримінального правопорушення, а й на основі криміналістичного аналізу їх окремих обставин» [154, с. 19].

Також в розрізі зазначеного вважаємо доречним навести твердження В. В. Лисенка, який вказує на те, що значення криміналістичної характеристики має практичне призначення не лише у випадку встановлення типових зв'язків між її елементами. Автор зазначає, що вказана категорія

може бути також ефективно застосована у діяльності правоохоронних органів за наявності нетипових особливостей окремих елементів чи зв’язків. Наостанок науковець зробив висновок, що до змісту криміналістичної характеристики необхідно включати інформацію про кримінальні правопорушення, яка має одиничні прояви, адже зазначені нетипові прояви злочинної діяльності можуть мати поширення у майбутньому [81, с. 234].

В свою чергу, окрема група вчених-криміналістів (В. В. Пясковський, Ю. М. Чорноус, А. В. Самодін) визначають криміналістичну характеристику кримінальних правопорушень яке систему узагальнених даних про найбільш типові ознаки певного виду (групи) кримінальних правопорушень, закономірний взаємозв’язок яких слугує основою наукового і практичного вирішення завдань розслідування [70, с. 579]. Зі свого боку, Г. А. Матусовський зауважує, що досліджувана наукова категорія, як накопичення та джерело відомостей про певні види кримінальних правопорушень, виконуючи інформаційну функцію, становить собою єдину інформаційну систему. Дослідник вірно акцентує увагу на тому, що використання останньої можливо шляхом одержання й аналізу відомостей щодо окремих елементів і встановлення зв'язків між ними, адже у цьому розумінні всі елементи системи теоретично рівнозначні і поділяти їх на основні та другорядні недоцільно. У той же час, Г. А. Матусовський зауважує, що використання такої інформаційної системи вимагає в кожному конкретному випадку виокремлення ключового елемента, через який можна здійснити «вхід» у систему з метою одержання необхідної інформації. Автор досить точно зазначає, що виокремлення ключового елемента для конкретного випадку залежить від конкретної слідчої ситуації, що склалася на даному етапі розслідування, а також від того, які вихідні дані має уповноважена особа та які з них необхідно встановити [91, с. 149].

Цікавою в розрізі вказаного попередніми авторами вважаємо думку А. Ф. Волобуєва, який засвідчує те, що «…криміналістична характеристика як кримінально-правова й кримінологічна містить у собі інформацію про

злочин у цілому, а також елементи, що його складають (об’єкт і об’єктивну сторону, суб’єкт і суб’єктивну сторону). На відміну від інших характеристик вона являє собою, по-перше, систему тільки криміналістично значимих відомостей про ознаки злочину, а не будь-яких однакових для всіх видів злочинів. У межах певного виду вони можуть сприяти його розкриттю. По-друге, відомості про ознаки елементів злочину описують на якісно-кількісному рівні. Таким чином підвищується практичне значення даної категорії криміналістики» [17, с. 32]. Як бачимо, автор в структуру визначеної наукової категорії в криміналістичному контексті включає як кримінально-правові, так і кримінологічні характеристики.

Досить влучним вважаємо твердження В. Д. Берназа, який вказував на те, що без опрацювання великого масиву кримінальних проваджень не представляється можливим визначити систему узагальнених відомостей групи протиправних діянь. З огляду на це, автор сформулював наступне визначення криміналістичної характеристики – «…це основана на державних статистичних даних науково-обґрунтована система узагальненої інформації та їх джерел про обставини, які були доказані, та інші, які мали значення для попередження, виявлення, розслідування та судового розгляду досліджуваних злочинів зазначеної категорії» [9, с. 17]. В свою чергу, М. М. Єфімов, даючи формулювання досліджуваної наукової категорії зробив це наступним чином: «…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» [35, с. 14-15].

А вже А. В. Старушкевич зазначає, що «…однією з причин неефективної боротьби з окремими видами злочинів є недостатнє дослідження саме криміналістичного аспекту пошуково-пізнавальної діяльності. Невипадково слідчі одностайно зазначають, що наявні у їх розпорядженні методичні рекомендації мають суттєві недоліки, не вміщують у достатньому об'ємі інформації, що необхідна для їх практичної діяльності.

Все це висуває вказану багатопланову проблему в коло актуальних напрямків, як теоретичних, так і прикладних криміналістичних досліджень. До вказаних досліджень і слід віднести роботи, пов'язані з розробкою теоретичних засад криміналістичної характеристики; формуванням криміналістичних характеристик окремих видів злочинів і їх використання для оптимізації попереднього слідства, підвищення його ефективності» [146, с. 3-4]. Тобто науковець наголошує на важливості зведення методичних рекомендацій практичним підрозділам до сухої алгоритмізації їх діяльності.

Зі свого боку, В. Ю. Шепітько доречно говорить про те, що «…криміналістична характеристика злочинів – досить нова наукова категорія криміналістики, яка посідає центральне місце в методиці розслідування окремих видів злочинів. Криміналістична характеристика — це результат наукового аналізу та узагальнення типових ознак певного виду або роду злочинів. Вона відображає злочин і його складові елементи. Крім криміналістичної характеристики злочинів, існують кримінально-правова, кримінально-процесуальна, кримінологічна характеристики. Криміналістичною характеристикою називається система відомостей про криміналістично значущі ознаки злочинів даного виду, що відображає закономірні зв’язки між ними і слугує побудові та перевірці слідчих версій у розслідуванні злочинів. Її метою є оптимізація процесу розкриття і розслідування злочину. Призначення криміналістичної характеристики полягає в тому, що вона сприяє: 1) розробленню окремих методик розслідування; 2) побудові типових програм і моделей розслідування злочинів; 3) визначенню напряму розслідування конкретного злочину. Ця характеристика слугує слідчому своєрідною інформаційною базою, набором відомостей про даний вид злочинів» [72, с. 274].

В той же час, В. Л. Синчук, на нашу думку, досить точно та правильно вказує на те, що практичне значення криміналістичної характеристики зводиться до того, що «…вона є робочим інструментом слідчого, який він може використати у процесі розслідування конкретного злочину на підставі

порівняння отриманих відомостей з тими типовими, що відображені у криміналістичній характеристиці і притаманні саме цьому виду злочинної діяльності» [132, с. 9]. Як бачимо, автор засвідчує те, що для досліджуваної наукової категорії головним є побудова правильних кореляційних зв'язків, які будуть допомагати уповноваженим особам у плануванні розслідування кримінальних правопорушень та проведенні окремих слідчих (розшукових) дій, а також інших процесуальних заходів.

Зі свого боку, О. Ю. Довженко, опрацьовуючи криміналістичну характеристику кіберзлочинів, зазначив, що «…в праві та доктрині найбільшого визнання серед багатьох альтернативних термінів набув термін «кіберзлочин», проте визначення поняття кіберзлочину досі відсутнє. На підставі аналізу літератури визначається, що кіберзлочин доцільно характеризувати через категорію кіберпростору. Визначається, що на заваді дослідженню та класифікації кіберзлочинів, та врешті створенню єдиного визначення кіберзлочинів в кримінальному праві стає недостатня концептуальна розробленість самого поняття кіберзлочину та розмитість «кордонів» між кіберзлочинами та рештою злочинних посягань. Шлях до розв'язання цієї проблеми вбачається в використанні концепції кіберпростору як особливої реальності, що створюється електронними технологіями та за допомогою комп'ютерних мереж. Це нематеріальний простір, що виникає на базі матеріальних об'єктів, таких як електронне обладнання, однак сам не є цими об'єктами, а є цифровим відображенням впливів, що здійснюються за допомогою предметів матеріального світу. Кіберпростір набуває все більше значення для людства, оскільки він відкриває нові можливості, тому слід очікувати його подальшого розширення. Кіберзлочин відрізняється від звичайного злочину тим, що існує в кібернетичному світі. За допомогою кіберпростору можливі практично будь-які види злочинного впливу, що можуть бути охарактеризовані в категоріях звичайного злочину, аж до нанесення тілесних ушкоджень чи вбивства. Саме використання віртуального простору кіберсвіту відділяє кіберзлочини від подібних ним злочинів, що

відбуваються в матеріальному просторі» [24, с. 5-6].

Доречною також вважаємо позицію Б. Є. Лук'янчикова, Є. Д. Лук'янчикова та С. Ю. Петряєва, які відмітили з прифоду формулювання поняття досліджуваної наукової категорії, що «…це інформаційна модель типових зв'язків і закономірно сформованих джерел інформації, яка дозволяє прогнозувати оптимальний шлях та ефективні засоби розслідування окремих видів (груп) злочинів. В науковому плані криміналістична характеристика є концепцією, основою побудови описової моделі певних видів (груп) злочинів з метою розробки відповідних методик їх розслідування. Новизна цієї категорії виявляється в системному відтворенні відомостей про криміналістично значущі ознаки певного виду (групи) злочинів. До її появи відомості про ознаки злочину викладалися непослідовно, їх коло було постійним, у деяких окремих методиках частина цих даних зовсім була відсутня. Застосування криміналістичної характеристики як інформаційної моделі дозволило систематизувати ці відомості у вигляді послідовно розташованих елементів, що мають певні кореляційні зв'язки. Саме в криміналістичній характеристиці на основі аналізу узагальнених відомостей про ознаки окремого виду злочинів виявляються закономірності, що належать до предмета дослідження науки криміналістики» [85, с. 209].

А вже інша група науковців вказала, що «…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» [71, с. 507].

Найбільш докладним вважаємо твердження колективу вчених-криміналістів, які відмітили, 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.... Криміналістична характеристика – сукупність взаємозалежних даних про криміналістично вагомі ознаки злочинів даного виду (групи), які сприяють їх розкриттю і розслідуванню шляхом побудови версій та їх перевірки в результаті проведення запланованих слідчих (розшукових) дій та інших заходів» [69, с. 346, 349].

З огляду на вищезазначене, можемо зробити висновок, що криміналістична характеристика правопорушень, пов’язаних з використанням інтернет-банкінгу, – це сукупність даних, отриманих із судово-слідчої практики, про криміналістично значимі ознаки певної категорії протиправних діянь, яка зводиться до кореляційних зв’язків між ними та забезпечує побудову і перевірку криміналістичних версій для вирішення основних завдань кримінального провадження, а також надає додаткову інформацію, необхідну для ефективного проведення слідчих (розшукових) дій.

Також слід зауважити, що для визначеної наукової категорії головним є побудова правильних кореляційних зв’язків, які будуть допомагати уповноваженим особам у плануванні розслідування кримінальних правопорушень та проведенні окремих слідчих (розшукових) дій, а також інших процесуальних заходів.

Питання правильного формування структури криміналістичної характеристики правопорушень завжди викликало суперечності між вченими-криміналістами. Тому зрозуміло, що при побудові окремої методики

ми також вирішили його дослідити.

Структура криміналістичної характеристики правопорушень завжди викликала та буде викликати суперечки між вченими-криміналістами. Це пов’язано з тим, що існують різні думки окремих груп науковців з приводу наявності різних елементів у вказаній структурі. Але в той же час майже усі дослідники погоджуються з необхідністю розроблення кореляційних зв’язків між ними, а також з наявністю наступних обов’язкових її складових: спосіб вчинення злочину, обстановка вчинення злочинів, слідова картина та особа злочинця. Тому визначення структури криміналістичної характеристики правопорушень, пов’язаних з використанням інтернет-банкінгу, а також надання опису ознак та властивостей окремих її елементів є важливим завданням в розробці визначеної методики розслідування [133, с. 127].

Наприклад, А. Ф. Волобуєв, опрацьовуючи методику розслідування розкрадань майна у сфері підприємницької діяльності, зауважив, що її криміналістична характеристика має відображати традиційні елементи, але з урахуванням власної специфіки, яку накладає на них підприємницька діяльність, зокрема: «…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)» [17, с. 35].

З приводу зазначеного окремі науковці вказують наступне: «…одним із найбільш дискусійних в теорії криміналістичної характеристики кримінальних правопорушень є питання про кількісний і якісний склад елементів, тобто криміналістично значимих ознак, які повинні складати ядро криміналістичної характеристики. До основних елементів криміналістичної характеристики певного виду (групи) кримінальних правопорушень слід віднести тільки елементи, що відрізняються чітким пошуково-розшуковим спрямуванням, й до них належать: – характеристика предмету злочинного посягання (речі матеріального світу, на які спрямоване посягання – гроші, цінності, майно тощо); – типові способи вчинення кримінального правопорушення (складаються зі способів підготовки, безпосереднього вчинення кримінального правопорушення та способів приховування (маскування) вчинених дій); – типова «слідова картина» події (комплекс матеріальних та ідеальних слідів, що притаманні певному виду (групі) кримінальних правопорушень та певним способам й етапам його вчинення); – характеристика особи підозрюваного (характеризується фізичними, соціально-демографічними даними; чинниками, що мали вплив на формування і здійснення протиправної мети, створення злочинної групи, розподілу ролей між співучасниками тощо); – характеристика особи потерпілого (демографічні дані, відомості про спосіб життя, риси характеру, звички, зв’язки і стосунки, ознаки віктимної поведінки тощо); – мотив та мета вчинення кримінального правопорушення (мотив – це внутрішнє спонукання, рушійна сила вчинку людини, що визначає його зміст і допомагає більш глибоко розкрити психічне ставлення особи до вчиненого; мета – це уявлення про бажаний результат, якого прагне особа, що визначає спрямованість діяння)» [70, с. 580].

Зі свого боку, С. В. Самойлов сформував наступну систему криміналістичної характеристики шахрайств, учинених із використанням мережі «Інтернет», а саме: «…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» [128, с. 7].

У свою чергу, В. Ю. Шепітько відмічав, 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 [72, с. 274].

А вже окрема група науковців (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) визначили наступні складові криміналістичної характеристики протиправних діянь у сфері інформаційних технологій: предмет безпосереднього посягання, спосіб вчинення злочину, слідова картина, особа злочинця та потерпілі [85, с. 469-472].

Зі свого боку, А. В. Іщенко в структурі криміналістичної характеристики правопорушень виокремлював наступні елементи: «…слідова картина, спосіб учинення злочину, предмет злочинного посягання, дані щодо особи злочинця та особи потерпілого» [47, с. 181].

Наступною позицією, яка відображає основні елементи досліджуваної наукової категорії буде позиція групи науковців, які серед них виокремили такі, як-от: «…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» [71, с. 507].

Інша група вчених-криміналістів також спробувала визначити структуру криміналістичної характеристики таким чином: «…1) сліди злочину; 2) спосіб вчинення злочину; 3) предмет злочинного посягання; 4) особистість злочинця; 5) обстановка вчинення злочину; 6) особистість потерпілого [69, с. 350].

Досить цікавою, на нашу думку, є позиція Т. В. Коршикової, яка серед елементів криміналістичної характеристики шахрайств, учинених з використанням електронно-обчислювальної техніки, визначила наступні: «…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» [65, с. 129].

В свою чергу, А. І. Кунтій зауважив, що «…у структурному плані криміналістична характеристика злочину, вчиненого у сфері використання ЕОМ, охоплює чотири основні елементи: 1) спосіб учинення злочину; 2) предмет безпосереднього посягання; 3) типові сліди злочину; 4) особа злочинця» [71, с. 867].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було визначено наступний перелік основних елементів криміналістичної характеристики правопорушень, пов’язаних із використанням інтернет-банкінгу:

– спосіб вчинення правопорушення;

– обстановка вчинення правопорушення;

– слідова картина протиправного діяння;

– особа правопорушника;

– особа потерпілого [135, с. 22].

Підсумовуючи, зазначимо, що криміналістична характеристика правопорушень, пов’язаних із використанням інтернет-банкінгу, є важливою складовою методики розслідування вказаних діянь. Адже вірно сформована структура визначеної наукової категорії дозволить виокремити найбільш чіткі кореляційні зв’язки, які допоможуть як в побудові криміналістичних версій, так і в ефективному проведенні окремих процесуальних дій.

1.3. Характеристика окремих елементів криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу

Надамо окремим з них характеристику їх ознак та властивостей. З приводу першого елементу, визначеного в наведеній вище системі криміналістичної характеристики, то у переважній більшості випадків (99 %) [Додаток Б] мають місце повноструктурний склад способу вчинення протиправних дій.

Для прикладу, стосовно способу вчинення протиправного діяння, то ми поділяємо позицію Н. В. Павлової, яка зауважує, що спосіб вчинення правопорушення є центральним в криміналістичній характеристиці, адже за його допомогою можна опрацювати виявлені у процесі аналізу зв'язки між всіма структурними елементами досліджуваної наукової категорії [103, с. 20]. Ми також вважаємо, що спосіб є центральним елементом криміналістичної характеристики. В умовах діджиталізації суспільства злочинна діяльність видозмінює свої форми та методи, злочинці дедалі використовують складні й нетипові способи учинення та приховання злочинних дій.

А вже В. А. Журавель говорить, що потрібно застосовувати функціональний аспект поведінки правопорушника для характеристики способу вчинення протиправного діяння як системи дій, прийомів, операцій, що спрямовані на досягнення певного злочинного результату. Автор наголошує на тому, що знання типових способів вчинення кримінальних правопорушень дозволяє ефективно застосовувати одну з найбільш ефективних та практичних схем розслідування їх, яка представляється науковцями у послідовності: від слідів правопорушення – до способу його вчинення; від способу вчинення – до особи правопорушника [39, с. 28].

Зі свого боку, С. М. Зав'ялов вказує на те, що спосіб вчинення протиправного діяння – це тріада способів готування, вчинення та його

приховання. Як влучно зазначає дослідник, «…ними виступає різновид діяльності людини, якій притаманні соціально-психологічні якості, орієнтувальні, сенсомоторні особливості суб'єкта» [40, с. 5]

В свою чергу, Т. В. Охрімчук відмічає, що основним елементом криміналістичної характеристики шахрайства з фінансовими ресурсами є спосіб його вчинення, який відповідно складається з системи взаємопов'язаних дій щодо підготовки, вчинення та приховування слідів кримінального правопорушення. Крім того, авторка поставила правильний акцент на тому, що спосіб вчинення досліджуваного протиправного діяння «…полягає, перш за все, в обмані, в наданні завідомо недостовірної інформації, зокрема, шляхом подання підроблених документів кредитору» [100, с. 95].

Доречною вважаємо також думку О. Л. Мусієнко, який наголошує на тому, що способи шахрайства характеризуються таким набором засобів і методів, які дозволяють вчинити обман настільки переконливо, що породжують щиру довіру потерпілого, через яку й відбувається передача майна. Крім того, автор вказує на факти типових для більшості шахрайських операцій етапів вчинення протиправних діянь «…охоплюють підготовку до проведення шахрайської операції, у тому числі розробку її схеми, здійснення необхідних організаційних і технічних заходів, безпосереднє вчинення обманних дій, заволодіння майном або правом на нього, а також ухилення від кримінальної відповідальності» [96, с. 151].

Ми підтримуємо окрему групу вчених-криміналістів, які сформулювали спосіб вчинення кримінального правопорушення як спосіб дій з готування, вчинення та приховання його слідів, що характеризує криміналістично значимі відомості про виконавця і застосовані ним засоби та можливості їх використання у розкритті та розслідуванні протиправних діянь [16, с. 27]. Тобто способи досліджуваної категорії протиправних діянь мають глибокі грані, які виявляються у сукупності взаємопов'язаних дій з підготовки, безпосереднього вчинення та їх приховування. Дані стосовно вказаних

способів є найбільш інформативним джерелом у кримінальному провадженні.

Першою складовою способу є підготовка до вчинення протиправного діяння. Відносно вказаного елементу, вважаємо доречною думку О. В. Баланюка, який її характеризує наступним чином: «…– підготовчі дії щодо приховування особистої участі (розроблення плану зі створення неправдивого алібі, що включає в себе комплекс дій, спрямованих на створення в певних осіб неправильного уявлення про істинне місце перебування злочинця в конкретний час, попередню домовленість із неправдивими свідками та інше; - підбір, придбання засобів, призначених для знищення слідів злочинця, а також підбір засобів, призначених для утруднення використання службово-пошукового собаки та інше); –підготовчі дії з приховання злочину в цілому і маскування окремих його обставин (виготовлення чи складання підроблених документів з метою приховання злочинних фінансово-господарських операцій чи справжніх обставин події; планування і підбір засобів та створення умов для вчинення інсценування події та інше); – підготовчі дії зі створення умов для ухилення від відповідальності і продовження злочинної діяльності (вчинення дій, спрямованих на створення уявлення про винність у злочині інших осіб, або «об'єктивних» обставин, що призвели до злочинних наслідків; вербування і установка корумпованих зв'язків із відповідними посадовими особами органів влади і управління та інше)» [6, с. 195-196].

В свою чергу, С. В. Чучко визначив наступні способи підготовки до вчинення шахрайства під час купівлі-продажу в мережі Інтернет: «…визначення найменування товару, що пропонуватиметься для продажу, створення його характеристик та отримання презентабельних фотографій; реєстрація та створення облікового запису особи в інформаційній телекомунікаційній системі під вигаданими анкетними даними; розміщення даних про товар; створення рівня довіри у покупців шляхом здійснення успішних цивільно-правових дистанційних угод та заповнення шкали

позитивних оцінок; створення «окремої» електронної адреси для здійснення переписки із потенційним споживачем; придбання «окремого» телефонного номеру для здійснення переговорів із потенційним споживачем; обрання способу здійснення розрахунків; реєстрація «електронних гаманців» у відповідних сервісах або отримання платіжної картки для перерахування грошей тощо» [172, с. 57].

Доречним в розрізі зазначеної інформації вважаємо думку А. І. Кунтія, який вказував, що протиправні діяння в сфері ЕОТ учиняються з попередньою підготовкою. Серед заходів такої підготовки автор виокремив такі, як-от: «…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)» [71, с. 867].

А вже Т. В. Коршикова стосовно підготовчих дій до визначених протиправних діянь, вирізняє такі: «…1) вчиненню шахрайства сприяв несанкціонований доступ до ЕОТ; 2) вчинення шахрайства здійснювалось з використанням шкідливих програмних чи технічних засобів; 3) вчиненню шахрайства сприяло розповсюдження рекламної чи іншої продукції про предмет посягання (надання послуг)» [65, с. 132].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] було визначено наступний 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..

З приводу безпосереднього способу вчинення визначеної групи кримінальних правопорушень вважаємо за необхідне вказати наступне. Наприклад, С. М. Зав'ялов доречно вказував на те, що реалізація сформованого злочинного наміру, що втілюється в окремих практичних діях суб'єкта займає велику частину способу вчинення злочину. Крім того, науковець зауважував, що реалізуючи злочинний намір, зловмисник опановує та аналізує низку обставин, за яких має діяти, зважає на можливості осіб, з якими планує вчинити злочин. З огляду на зазначене, автор підсумував, що на вказаному етапі правопорушник окреслює план своїх дій, обмірковує послідовність виконання деяких з них, готує знаряддя та засоби вчинення протиправного діяння, обирає спосіб їх застосування, продумує усунення певних перешкод, способи маскування слідів [41, с. 37].

Опрацювання окремих праць вчених-криміналістів стосовно досліджуваної тематики (С. В. Самойлова [129], О. А. Самойленко [126], О. В. Кришевича [78]), дозволило зробити висновок, що способи вчинення визначеної категорії протиправних діянь можуть бути досить різноманітними та акумулювати у собі різні склади кримінальних правопорушень, передбачених КК України.

Для прикладу, наведемо наступну ситуацію: гр. А., перебуваючи у трудових відносинах з РФ ПАТ КБ «Приватбанк», обіймаючи посаду касира-операціоніста, діючи з корисливих мотивів, маючи умисел на привласнення та розтрату грошових коштів Банку, які були їй ввірені та перебували в її віданні, в період часу з 15 лютого 2012 року по 27 червня 2012 року привласнила та розтратила грошові кошти, шляхом безпідставного сторнування операції переказу коштів, спричинивши при цьому матеріальних збитків РФ ПАТ КБ «Приватбанк» на загальну суму 54 957,18 гривень. Зокрема, 11 червня 2012 року о 15 годині 00 хвилин, знаходячись на своєму

робочому місці, при виконанні службових обов'язків, гр. А. отримала грошові кошти від гр. Б. в сумі 20000 гривень, які привласнила та розтратила, шляхом безпідставного сторнування операції переказу коштів, спричинивши при цьому матеріальних збитків РФ ПАТ КБ «Приватбанк» на вказану суму. Крім того, керуючись єдиним злочинним умислом, правопорушниця 24 квітня 2012 року о 16 годині 30 хвилин, знаходячись на своєму робочому місці, при виконанні службових обов'язків, отримала грошові кошти від гр. В. в сумі 11500 гривень, які знову привласнила та розтратила. Таку саму діяльність гр. А реалізовувала ще декілька раз [142].

Раціональною також вбачаємо позицію І. О. Коваленка, який основними способами вчинення шахрайства в сфері банківських електронних платежів в Україні виділяв такі як: «…фішинг; сніфферінг; вішинг; кардінг» [52, с. 139]. В розрізі зазначеного вважаємо доцільним приведення для ознайомлення Міжнародну класифікацію та коди комп'ютерних злочинів, яку надав А. І. Кунтій, як-от: «QA – Втручання або перехоплення. QAH – Незаконний доступ. QAI – Перехоплення. QAT – Викрадення часу. QAZ – Інші випадки несанкціонованого доступу або перехоплення. QD – Зміна або пошкодження інформації. QDL – «Логічна бомба». QDT – «Троянський кінь». QDV – Програми-віруси. QDW – «Черв'яки». QDZ – Інші випадки пошкодження інформації. QF – Комп'ютерне шахрайство. QFC – Шахрайство з автоматами по видачі готівки. QFF – Комп'ютерна підробка. QFG – Шахрайство з ігровими автоматами. QFM – Шахрайство шляхом неправильного вводу/ виводу або маніпуляції програмами. QFP – Шахрайство з платіжними засобами. QFT – Телефонне шахрайство. QFZ – Інші випадки комп'ютерного шахрайства. QR – Несанкціоноване копіювання. QRG – Несанкціоноване тиражування комп'ютерних ігор. QRS – Несанкціоноване тиражування програмного забезпечення. QRT – Несанкціоноване тиражування напівпровідникової продукції. QRZ – Інші випадки несанкціонованого копіювання. QS – Комп'ютерний саботаж. QSH – Саботаж технічного забезпечення. QSS – Саботаж програмного забезпечення. QSZ – Інші види

комп'ютерного саботажу. QZ – Злочини, пов'язані з комп'ютерами. QZB – Незаконне використання дошки електронних оголошень (BBS). QZE – Викрадення комерційної таємниці. QZS – Зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування. QZZ – Інші випадки вчинення злочинів, пов'язаних із комп'ютерами» [71, с. 892-893].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] було виокремлено такий перелік способів безпосереднього вчинення досліджуваної категорії кримінальних правопорушень:

1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг);

2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;

3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення;

4) розповсюдження шкідливих програмних чи технічних засобів або їх збут з використанням мережі Інтернет;

5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах;

6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін..

Відносно окремих аспектів приховування, то, наприклад, В. К. Весельський, С. М. Зав'ялов і В. В. Пясковський виокремлювали серед них наступні групи: «…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» [16, с. 37].

А вже І. О. Коваленко вказував, що «…шахраї використовували наступні способи приховування своєї протиправної діяльності: використання зміни ідентифікатора місця знаходження свого обладнання; знищення обладнання, яке використовувалось для вчинення кримінальних правопорушень; надання неправдивих показів під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів; відмова від дачі показань» [55, с. 146].

Для прикладу, гр. Ю., маючи навики роботи з програмним забезпеченням для користування всесвітньою мережею Інтернет, використовуючи невстановлену досудовим розслідуванням електронно-обчислювальну машину (комп'ютер), маючи умисел на створення з метою збуту та збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу ЕОТ, усвідомлюючи суспільно небезпечний характер своїх дій, завантажив у невстановленого користувача всесвітньої мережі Інтернет файл з назвою «Revenge-RAT v.0.2.exe» (програма з автоматичним прихованим встановленням, яка надає можливість віддаленого керування комп'ютерами і прихованого спостереження за їх користувачами), а також в якому присутні різноманітні налаштування, які додаються при створенні кінцевого файлу. В подальшому, гр. Ю. шляхом модифікації існуючого програмного засобу, створив з метою збуту шкідливе програмне забезпечення під назвою «Revenge-RAT v.0.2.exe» (інфіковане вірусом типу «Trojan») невидиме для антивірусів, призначене для несанкціонованого втручання в роботу ЕОТ. Після цього правопорушник, з метою приховування створеного ним шкідливого програмного забезпечення, за допомогою легального інстальованого програмного забезпечення – архіватора «WinRAR», помістив файл з назвою «Revenge-RAT v.0.2.exe» до архіву під назвою «teamviewer.rar». 10.12.2018 року гр. Ю., керуючись корисливим мотивом, з метою незаконного збагачення, за допомогою всесвітньої мережі Інтернет, шляхом надсилання електронного листа, збув

гр. О. шкідливі програмні засоби (забезпечення) типу «Trojan», призначені для несанкціонованого втручання в роботу ЕОТ [141]. Як бачимо, гр. Ю. для приховування створеного шкідливого програмного забезпечення, за допомогою легального інстальованого програмного забезпечення (архіватора «WinRAR»), помістив файл з назвою «Revenge-RAT v.0.2.exe» до архіву під назвою «teamviewer.rar».

Стосовно приховування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, на основі дослідження опитування респондентів [Додаток Б] було з'ясовано такі заходи:

– знищення обладнання, що використовувалось для вчинення протиправних дій – 41 %;

– приховування створеного шкідливого програмного забезпечення за допомогою легального програмного забезпечення – 44 %;

– використання перетворення ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються протиправні дії – 78 %;

– дача неправдивих показів при проведенні окремих процесуальних дій (в тому числі – неправдиве алібі) – 31 %;

– відмова від дачі показань – 65 %.

Підводячи підсумок, зазначимо, що нами було удосконалено систему способів безпосереднього вчинення досліджуваної категорії кримінальних правопорушень, а також опрацьовано способи підготовки та приховування визначених протиправних діянь.

Ведучи мову про обстановку вчинення кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, зважаємо за потрібне зупинитись на формулюванні її визначення. Наприклад, В. В. Тіщенко вдало наголошує на тому, що вчинення протиправного діяння, як і будь-яка інша складна система, випливає з обстановкою його вчинення та дій правопорушника. Науковець зауважує, що «…злочинець вчинює, а також у разі наявності готує та приховує злочин у конкретних умовах обстановки. Відповідно, зловмисник може зайняти активну або пасивну позицію. При

активній позиції суб'єкта він не тільки враховує конкретну обстановку в динаміці сприятливих і несприятливих факторів, але й намагається змінити її, створити такі умови, які сприяли б здійсненню його злочинного задуму та приховуванню злочину. Пасивна позиція злочинця автором визначається як сукупність умов, що складаються поза його волею і на які він впливати не може. При плануванні злочину особа оцінює обстановку, з'ясовує та аналізує умови, що сприяють або перешкоджають реалізації його намірів. Оскільки умови, в яких перебуває об'єкт, що цікавить злочинця, є динамічними у тому чи іншому ступені, і він намагається підібрати для здійснення його задуму найбільш сприятливі» [155, с. 84].

Для прикладу, в ранковий час 04.10.2018 гр. П., перебуваючи за у себе вдома, використовуючи власний персональний комп'ютер та під'єднавшись до мережі загального доступу Інтернет, використовуючи засіб маршрутизації Wi-fi-роутер «TP-Link» виявив web-сайт за посиланням http://www.stolstul.com.ua. В цей день, час, місці та за вказаних обставин у останнього виник злочинний умисел, направлений на порушення роботи виявленого інтернет-ресурсу. З цією метою гр. П., відкрив «панель розробника», використовуючи web-браузер, та розпочав пошук вразливостей web-сайту. Продовжуючи реалізацію свого злочинного умислу, маючи власний досвід у створенні програмного забезпечення на мовах програмування, правопорушник виявивши форми зворотного дзвінка «callback» та форму зворотного зв'язку, в текстовому редакторі «Блокнот» створив сценарій (скрипт) для виконання автоматизованого завдання, а саме масового надсилання електронних повідомлень на отримання зворотного дзвінка гр. О. та зворотного зв'язку. З метою доведення свого злочинного умислу до кінця, гр. П., відкривши форму «замовлення товару», здійснив заповнення полів та, не бажаючи, щоб злочинні дії останнього було викрито, використовуючи засоби анонімізації, змінив IP-адресу [144]. Як бачимо, протиправне діяння було вчинено в ранковий час за місцем проживання особи злочинця.

Доцільною також вбачаємо позицію Б. В. Черняховського, який засвідчує, що «…середовище вчинення злочину, пов'язаного із застосуванням комп'ютерних технологій, умовно можна поділити на матеріальне (комп'ютерно-технічне устаткування, приміщення, у якому воно знаходиться) і нематеріальне інформаційне середовище в цифровій (електронній) формі» [167, с. 59].

Зі свого боку, В. В. Апопій досліджуючи питання е-торгівлі, акцентує увагу на повністю безконтактному способі спілкування між особою злочинця та потерпілим Автор наголошує, що «…за змістом своєї діяльності інтернет-торгівля сильно відрізняється від звичайної роздрібної торгівлі. Їй властиві певні функції та особливості, серед яких основними є: віртуальність, тобто відсутність особистого контакту між окремими особами – учасниками процесу купівлі-продажу; інтерактивність, тобто адекватне інформаційне забезпечення покупця його запиту у вигляді беззвучного діалогу; глобальність, тобто відсутність часових, просторових, адміністративних, соціально-демографічних, асортиментних кордонів; динамічність, тобто здатність онлайн-торгівлі до моментальних змін та адаптації до нових умов; ефективність, тобто здатність забезпечувати прибуток, інші економічні вигоди та соціальний ефект» [4, с. 27]. Тобто обстановку вчинення протиправного діяння можна характеризувати обставинами місця та часу, що в більшості випадків є невизначеними, адже обіймають велику кількість об'єктів, що можуть бути місцем події.

Також доцільним вважаємо твердження О. І. Мотляха говорить про те, що проблеми вибору місця та часу правопорушником у здійсненні власних умислів зостається вкрай спірним серед вчених-криміналістів. На думку автора, серед вказаних місць можуть бути такі як: «…адміністративні та службові приміщення різного типу суб'єктів господарювання (підприємств, організацій, компаній, фірм тощо), які використовують у своїй виробничій діяльності операційні комп'ютерні системи та їх периферійні устаткування; власні та орендовані житлові приміщення (офіси, квартири, кімнати та інше),

в яких встановлені комп'ютери (комп'ютер), що забезпечені виходом до всесвітньої мережевої системи Інтернет; приміщення комунальної власності або ж споріднені з ними (цокольні, напівпідвальні чи ті, що примикають до житлових будинків приміщення), котрі на правах власності чи оренди можуть використовуватися під комп'ютерні клуби, інтернет-кафе тощо» [94, с. 64].

А вже С. В. Самойлов серед місць вчинення шахрайства в мережі Інтернет виділяє такі, як-от: «…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» [128, с. 8].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] було визначено наступні місця вчинення досліджуваної категорії кримінальних правопорушень:

– місця розташування електронно-обчислювальної техніки, з якої вчинялись протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 61 %;

– місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %;

– місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу – 12 %.

– інші – 6 %.

Підсумовуючи, можна визначити обстановку учинення кримінальних правопорушень як систему об'єктивних чинників й умов матеріальної обстановки, а також просторово-часових характеристик місця та часу.

Стосовно слідової картини то, для прикладу, С. М. Зав'ялов зауважував, що «…подія злочину – це один із матеріальних процесів дійсності, що

перебуває у зв'язку і взаємообумовлена з іншими процесами, подіями і явищами, відбивається в них і сама є відображенням якихось процесів. Будь-яка подія пов'язана зі змінами в навколишньому середовищі, і для того щоб дізнатися про подію злочину, необхідно виокремити пов'язані з ним зміни. Лише за слідами, які досліджуються в ході розслідуваної події, можна судити про його зміст» [40, с. 9]

А вже Т. В. Охрімчук підтверджувала те, що сліди шахрайства з фінансовими ресурсами у криміналістичній площині можуть визначатися з двох сторін: «…як особливості матеріальної шкоди, спричиненої вчиненням злочину; особливості механізму слідоутворення та змісту слідів (інформації). Авторка з'ясувала, що у цілому, слідова картина злочину, передбаченого ст. 222 КК України, визначена способом вчинення даного виду протиправного діяння та характеризується наявністю матеріальних та ідеальних джерел інформації. Тобто слідова картина злочину шахрайства з фінансовими ресурсами обумовлена способом вчинення злочину та характеризується наявністю матеріальних (документи різного виду та значення) та ідеальних (показання осіб, які володіють необхідними відомостями про обставини вчинення злочину) джерел інформації» [98, с. 372].

В свою чергу, Р. Л. Степанюк та С. І. Перлін акцентували увагу на тому, 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» [149, с. 288].

Досить вдалим вбачаємо твердження А. І. Анапольської, яка вказала, 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» [2, с. 165].

Зі свого боку, Х. І. Дуда зазначив, що «…слідова картина комп’ютерних злочинів дуже специфічна і вимагає розробки принципово інших методів і засобів в порівнянні з традиційними. Сліди вчинення даних злочинів рідко залишаються у вигляді видимих змін навколишнього середовища. Вони в основному не розглядаються сучасною трасологією, оскільки в більшості випадків носять інформаційний характер, тобто є тими або іншими змінами в комп’ютерній інформації, що виражається у формі її блокування, копіювання, модифікації, знищення. Скоєння особою протиправних дій, пов’язаних з використанням комп’ютерних технологій спричиняє виникнення певної кількості слідів у тому числі і специфічних, притаманних лише зазначеній категорії злочинів. Використання цих інформаційних даних при розслідуванні злочинів є необхідною умовою забезпечення всебічного, повного й об’єктивного дослідження обставин справи» [32, с. 263].

В розрізі опрацювання вказаного питання (слідової картини протиправних діянь) доречною вважаємо позицію А. С. Білоусова, який відмічав, що «…віртуальні сліди існують об’єктивно на матеріальних носіях, але не доступні для безпосереднього сприйняття. Для їх сприйняття потрібне обов’язкове застосування програмно-технічних засобів, отже наявність таких слідів на матеріальному носієві наближує цю групу до матеріальних слідів, але не робить їх такими. Отримані з матеріального носія і сприйняті віртуальні сліди внутрішньо не надійні завдяки природі їх існування, тому що їх можна неправильно прочитати, наприклад, застосувавши інші

програмно-технічні засоби, легко підробити, легко втратити. Це близько до суб'єктивного сприйняття і наближає такі сліди до ідеальних, але не може бути ототожненим з останніми. Віртуальні сліди зберігаються в ідеальному вигляді, але не в пам'яті людини, а в машинній пам'яті і на матеріальних носіях машинної інформації, їх виявляють з використанням технічних засобів у відповідності до певних алгоритмів» [12, с. 9].

Окрема група дослідників (Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан) у навчальному посібнику «Кіберзлочинність та електронні докази» доречно вказали, що «…в окремих слідчих ситуаціях, а саме, коли об'єкти сфери високих інформаційних технологій використовувались як засоби зв'язку злочинців, для розповсюдження порнографічних предметів, розміщення інформації про продажів заборонених товарів тощо, виникає необхідність надання статусу доказів інформації, яка розміщення в мережі Інтернет. На сьогодні, на фрагментарному рівні практикою вироблені окремі методи фіксації змісту web-сайту з метою подальшого використання у кримінальному судочинстві: роздруківка веб-сторінки через браузер; роздруківка та подання рапорту працівником поліції; огляд вебсайту слідчим у присутності понятих – аналогічний огляд разом зі спеціалістом; відповідь провайдера на запит щодо змісту сайту. З метою забезпечення допустимості «цифрових доказів» необхідно використовувати можливості сучасних судових техніко-криміналістичних експертиз, зокрема: експертизи комп'ютерної техніки і програмних продуктів, інформаційно-комп'ютерної експертизи та комплексної експертизи. При цьому увага експерта має зосереджуватися на виявленні ознак модифікації цифрової інформації, її способів та меж» [50, с. 138-139]. Вказана позиція знайшла своє відображення і в дисертаційному дослідженні А. Е. Жиліна, який підтвердив, що «за даними проведеного вивчення матеріалів кримінальних проваджень вказаний вид слідів наявний в 100 % кримінальних проваджень» [38, с. 67].

В свою чергу, Н. М. Ахтирська вказує, що «сліди вчинення кіберзлочинів можуть знаходитись не лише безпосередньо в комп'ютерній

техніці, на флеш-носіях, а і в кіберпросторі – середовищі (віртуальному просторі), яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних» [5, с. 138].

Досить правильною в розрізі дослідження кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, вбачаємо твердження Т. В. Коршикової, яка зазначила, що «Цифрові сліди шахрайств, учинених з використанням ЕОТ, можуть утворюватися: – на фізичних носіях комп'ютерної інформації (жорсткі диски, компакт-диски, флешкарти, накопичувачі інформації та ін.), якими користувався злочинець; – в оперативному запам'ятовуючому пристрої ЕОТ злочинця; – в оперативному запам'ятовуючому пристрої периферійних пристроїв злочинця; – в електронній поштовій скриньці злочинця (тут можуть міститися сліди переписки злочинця з потерпілим і, навпаки, а також переписка злочинця з іншими злочинцями); – на інтернет-сайті, який використовувався злочинцем з метою вчинення шахрайства; – як профіль у соціальних мережах злочинця («ВКонтакте», «Instagram», «Facebook», «Одноклассники», «Twitter» та ін.); – внаслідок проведення банківських платежів між потерпілим і злочинцем (рахунок в електронних платіжних системах («Qiwi-гаманець», Perfect Money та ін.); – під час зняття злочинцем у банкоматах коштів, отриманих злочинним шляхом» [63, с. 53].

Також досить точно С. С. Чернявський говорить про те, що «…перелік об'єктів, що зберігають слідову інформацію, умовно складається з шести груп: документи (письмові, графічні, фото-, кіно-, аудіо-, відео-, електронні); предмети (печатки, штампи, зразки бланків, платіжні картки); приміщення (офісні, складські, житлові); товарно-матеріальні цінності (рухоме, нерухоме майно) та гроші (готівкові та безготівкові); електронні носії інформації (комп'ютери, магнітні та лазерні диски); пам'ять людей. Визначено категорії документів, що мають доказове значення, виокремлено ознаки підроблення

документів (у 90,0 % справ мало місце підроблення документів, зокрема у 71,4 % – із застосуванням комп'ютерної техніки)» [165, с. 14].

Стосовно протиправних діянь визначеної категорії встановлено, що переважний масив слідової інформації залишається у мережі Інтернет (безпосередньо в проведених інтернет-операціях, в кеш-пам'яті або хмарних сховищах). Крім того, з'ясовано, що у більшості випадків потерпілий не має візуального контакту з правопорушником.

Підводячи підсумок, зазначимо, що кримінальним правопорушенням, пов'язаним із використанням інтернет-банкінгу, характерні електронні сліди (віртуальні, цифрові, комп'ютерні). Зазначені сліди переважно знаходяться в наступних місцях: акаунти, пам'ять електронно-обчислювальної техніки, профілі соціальних мереж, сайти для криптовалютних переписок, бази даних операторів зв'язку та інтернет-провайдерів, флеш-носії.

Особа правопорушника є одним з основних елементів майже всіх сучасних криміналістичних характеристик. Це пояснюється декількома факторами. 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 [136, с. 31].

Дану категорію вивчали науковці з різних галузей права – криміналістики, кримінології, кримінального права та інших суміжних галузей. Серед них ми вважаємо слушним виокремити таких як І. М. Даньшин [76], О. М. Джужа [77], В. В. Логінова [83], М. В. Салтевський, В. Г. Лукашевич, В. М. Глібко [125], О. Є. Михайлов, А. В. Горбань, В. В. Міщук [92], С. А. Шалгунова [173] та інші.

Щодо формулювання поняття особи злочинця як елементу криміналістичної характеристики для початку звернемося до позиції

О. Р. Лужецької, яка розглядає 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» [84, с. 200].

Доречною вбачаємо думку В. М. Плетенця, який наголошує, що встановлення особи – це складна діяльність, у ході якої з використанням криміналістичних методів і засобів відбувається виявлення, фіксація та дослідження інформативних властивостей й ознак людини, важливих для розслідування кримінального правопорушення. Автор вказує, що вивчення особи допоможе й у протидії розслідуванню. Оскільки, на думку дослідника, у відношенні особи, до якої застосовуватиметься раптовий характер дій, у першу чергу, слід знати її соціально-демографічні, психологічні та інші дані [106, с. 243].

А вже В. В. Бедь досліджуючи вказану проблематику, зауважив, що «…злочинна поведінка зумовлена взаємодією особистості з соціальним середовищем. Політичні, соціально-економічні, духовні сторони суспільства здійснюють зовнішній вплив на формування механізму злочину, а психічні особливості формують механізм злочину з середини. Крім того, вони зазначають, що психологія організованої злочинності відрізняється спільністю злочинних цілей та інтересів. Адже злочинна група створюється з метою здійснення не одного єдиного злочину, а для постійної і довготривалої злочинної діяльності» [8, с. 151].

Ми підтримуємо позицію Ю. А. Чаплинської, яка слушно констатує, що відомості про особу правопорушника дають змогу виокремити ті дані, що необхідні для організації найбільш ефективного розшуку особи, яка вчинила протиправне діяння, а в подальшому – її викриття, забезпечують усунення причин та умов вчинення кримінальних правопорушень та їх рецидивів.

Авторка відмічає, що в ході проведення слідчих (розшукових) дій вказані відомості надають можливість ефективного встановлення психологічного контакту, а також застосування відповідних тактичних прийомів [160, с. 181].

Окрема група вчених-кримінологів (Ю. Ф. Іванов, О. М. Джужа) виводять наступні групи відомостей, які характеризують особу правопорушника, а саме: 1) соціально-демографічні; 2) кримінально-правові; 3) моральні якості; 4) психологічні ознаки; 5) фізичні (біологічні) характеристики [46, с. 86-87].

Інша група науковців вказане поняття визначила таким чином: «…це сукупність соціальних властивостей, ознак, зв'язків і відносин, що характеризують особу, яка порушує кримінальний закон, і в поєднанні з іншими (не особистісними) умовами й обставинами спонукають особу до антисуспільної поведінки» [1, с. 78]. Інакше кажучи, вчені-кримінологи (Ю. В. Александров, А. П. Гель, Г. С. Семаков) сформулювали визначення особи правопорушника через виокремлення сукупності різних його властивостей та ознак.

Ми підтримуємо позицію О. Г. Кальмана з приводу того, що соціально-демографічна характеристика включає в себе відомості про стать, вік, сімейний стан, освіту, професію, наявність судимості тощо, визначає певний статус особи, визначений її належністю до певного класу (соціального прошарку) та до групи із соціально-демографічною характеристикою [49, с. 286].

Цікавою є позиція Д. О. Рички, який на основі власного дослідження визначив можливість виокремлення наступних груп осіб, які ймовірно можуть бути комп'ютерними злочинцям, як-от: «Перша група злочинців – особи, які використовують можливості комп'ютерних мереж та не належать ні до числа працівників організацій, ні до числа тих, хто займається сервісним обслуговуванням комп'ютерних систем. До другої групи належать працівники організації з законним доступом до устаткування, що входить до локальних та комп'ютерних телекомунікаційних мереж, а також особи, які не

є такими, але мають доступ до комп’ютерних систем по комп’ютерним мережам. До третьої групи належать працівники усіх рангів, навіть такі, що не мають глибоких знань у роботі комп’ютерних систем, але сприяють вчиненню комп’ютерного злочину. Четверта група – працівники, які згідно зі своєю посадою мають санкціонований доступ до приміщень з комп'ютерними системами та периферією і виконують на ЕОМ певні дії, що входять до їхніх обов’язків. П’ята група – це особи, які за родом своєї діяльності безпосередньо пов’язані з комп’ютерними системами або відповідають за функціонування та є працівниками такої організації. На нашу думку такі злочинці є найбільш обізнаними у комп’ютерних технологіях та, відповідно, є найнебезпечнішими з вищеперелічених осіб» [121, с. 121].

А вже І. О. Коваленко зробив правильний умовивід про те, що «…особа шахрая в кримінальних провадженнях за фактом вчинення шахрайства у сфері банківських електронних платежів характеризується наступними групами ознак: 1) загально-демографічні (стать, національність, вік); 2) соціальної ролі (вид занять, сімейний стан, належність до певних соціальних груп); 3) мотив, відношення до вчиненого протиправного діяння та поведінка в ході досудового розслідування; 4) рецидив діяння» [57, с. 84].

Підтримуючи більшу частину вищенаведених визначень та структур, нами було вирішено надати власний перелік ознак та властивостей, що характеризують особу, яка вчиняє кримінальні правопорушення, пов’язані з використанням інтернет-банкінгу, а саме:

– інтелектуальні та психологічні властивості, що загалом позначаються на побудові її криміналістичного портрету;

– соціально-демографічні ознаки та властивості (освіта, сімейний стан);

– моральні властивості (місце мешкання, вид діяльності, роботи, навчання);

– фізичні ознаки (стать, вік, фізичні дані).

Підсумовуючи, зазначимо, що особа, яка вчиняє досліджувані протиправні діяння, є важливою складовою криміналістичної

характеристики. Нами було надано перелік ознак та властивостей, які характеризують визначену категорію правопорушників.

Для прикладу, на підставі аналізу кримінальних проваджень [Додаток А] встановлено, що досліджувані протиправні діяння вчинюють переважно чоловіки (91 %). Стосовно критерію віку особи, яка їх вчинила, з'ясовано, що це були особи у віці 16-20 років – 8 %, 20-30 років – 42 %, 30-40 – 26 %, 40-50 років – 19 %, 50 років і старше – 5 %.

В свою чергу, Ю. М. Піцик, опрацьовуючи окремі аспекти особистості кіберзлочинця, вказує на те, що «…у порівнянні з традиційними видами шахрайства інтернет-шахрайство є досить «молодим» видом кримінального правопорушення. Згідно зі статистичними даними, більшість кіберзлочинів проти власності (79 %) – це шахрайства, учинені чоловіками (94 %). Такі злочини вчиняють здебільшого особи, які офіційно не перебувають у шлюбі та не мають дітей. Кількість неодружених осіб становить 70 %, одружених – 30 %. Згідно з даними судової практики, 51 % осіб, які вчинили кіберзлочини, не мають постійного місця роботи, такі особи вчиняють зазвичай шахрайства. Серед решти 49 % більшість становлять менеджери нижчої та середньої ланок, рідше – посадові особи та програмісти. Якщо середній вік шахрая в матеріальному світі становить 26–39 років, то середній вік кібершахрая – від 18 до 40 років. Соціальне становище в суспільстві – від студента до співробітника державної установи або фірми» [104, с. 106].

Відносно рівня освіти правопорушників [Додаток А] встановлено наступні дані: базову середню освіту має 1 % правопорушників, середню – 2 %, середню спеціальну – 4 %, базову вищу – 15 %, вищу – 79 %. Підсумовуючи зазначене, було створено ймовірний «портрет» особи правопорушника.

Окрема група дослідників (М. І. Стрюк, С. О. Семеріков, А. М. Стрюк) зауважує, що «…у кіберпросторі злочинець-користувач може бути суб'єктом багатьох соціальних спільнот (груп) у соціальних мережах, мати багато активних акаунтів (з англ. *account*) чи профілів, облікових записів, або ж

узагалі не мати потреби в цьому. Варто додати, що географічна мобільність не завжди пов'язана з професійною, адже людина може мати високий ступінь географічної мобільності без можливості змінити особистий вибір і компетентність (роз'їзна робота з низьким рівнем професійної, соціальної та економічної мобільності)» [152, с. 44].

За результатами узагальнення даних кримінальних проваджень [Додаток А] 85 % осіб, які вчиняють досліджувані протиправні діяння, відрізняються досить високим інтелектуальним рівнем.

В розрізі зазначеного вважаємо доречним твердження К. Д. Зайця, який вказує, 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. Шахраї даної категорії – це інтелектуально обдаровані особи, які бачать метою свого життя виявляти слабкості державної системи й законодавства, та користуватися ними для власного збагачення» [44, с. 8].

Підбиваючи підсумок, зауважимо, що кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу, в більшості вчиняють особи чоловічої статі віком 20-40 років, які мають вищу освіту, неодружені та відрізняються досить високим рівнем інтелекту.

Стосовно особи потерпілого, для початку 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» [172, с. 87].

Загалом, ми підтримуємо позицію М. В. Сенаторов, який сформулював в своєму монографічному дослідженні наступне поняття «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, С. В. Самойлов наголошує на тому, що для вивчення особи потерпілого усіх потерпілих поділено на дві категорії: 1) активних користувачів мережі, які постраждали внаслідок недобросовісного виконання обов'язків за договором купівлі/продажу (обміну); 2) користувачів, які мають невеликий досвід використання мережі та стали потерпілими внаслідок відсутності необхідних знань про заходи обережності в мережі «Інтернет». Також дослідник засвідчує, що «…серед потерпілих обох категорій наявні особи, які навмисно порушують вітчизняне законодавство чи законодавство інших країн» [128, с. 8].

Досить доречною вважаємо думку А. В. Рейнгольда, який відмічав, 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. Крім того, автор акцентував увагу на тому, що бажання швидкого придбання товару при мінімальних витратах та халатне відношення до обрання суб'єктів, які пропонують товари і послуги, може зробити кожного потенційним потерпілим. Дослідник на основі опрацювання судово-слідчої практик зробив висновок, що у 88 % випадків від дій шахраїв

страждає особа, яка виступає набувачем товарів та послуг (покупець). Також ми підтримуємо твердження науковця, що іноді потерпілим може стати не тільки покупець, а й продавець [116, с. 111].

В свою чергу, М. Ю. Литвинов вказує, 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» [80, с. 86].

Говорячи про особу потерпілого вважаємо за доцільне розглянути монографічне дослідження О. Л. Мусієнка, в якому автор відмічає, що «жертва злочину вивчається також у системі зв’язків, особистих стосунків, що склалися в найближчому соціальному оточенні (з рідними, близькими, друзями, знайомими). Виявлення своєрідності психології жертви (характеру, інтелекту, схильностей, інтересів, емоційних якостей та інших психічних особливостей), її положення в системі зв’язків і взаємин з іншими особами дозволяє простежити вчинення злочинного посягання в розвитку» [97, с. 81].

А вже опрацювання матеріалів кримінальних проваджень [Додаток А] дозволило вирізнити такі віктимогенні групи потерпілих, як-от:

а) працівники фінансових установ, підприємств та організацій різних форм власності;

б) клієнти фінансових установ, підприємств та організацій різних форм власності;

в) родичі клієнтів фінансових установ, підприємств та організацій різних форм власності.

Підводячи підсумок, зазначимо, що дослідження опису ознак та властивостей окремих елементів криміналістичної характеристики правопорушень, пов’язаних з використанням інтернет-банкінгу, є важливим завданням при побудові ефективної криміналістичної характеристики. Серед основних елементів вищевказаної наукової категорії було визначено наступні: спосіб вчинення правопорушення; обстановка вчинення правопорушення; слідова картина протиправного діяння; особа правопорушника; особа потерпілого.

Висновки до розділу 1

З огляду на опрацювання теоретичних засад побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, варто сформулювати наступні висновки:

1. Здійснено детальний аналіз протиправних діянь у сфері використання банківських електронних платежів та запропоновано їхню обґрунтовану класифікацію. Акцентовано увагу на «цифровізації» суспільства. Доведено, що на сьогодні термін «цифровізація» вживають у значно широкому розумінні, у тому числі і як «цифрову революцію» в економіці, суспільстві та приватному житті. Наголошено, що поняття «кіберзлочинів» утворилося у 1980-х роках після запуску в 1971 році комп'ютерного вірусу за назвою «Creeper» (дистанційна програма), який після потрапляння в комп'ютерну мережу залишав вислів: «Я – Повзун. Спіймай мене якщо зможеш». Зосереджено увагу на тому, що на протязі значного періоду протиправні діяння, що вчинялися за допомогою електронно-обчислювальної техніки, взагалі не характеризувались як кримінальне правопорушення.

2. Зазначено, що на початку 2000-х років законодавці у більшості країн Європейського Союзу дійшли висновків про необхідність виокремлення конкретних протиправних діянь, які можуть вчинюватися з використанням комп'ютерних систем (технологій). Вказані положення було закріплено у низці міжнародних нормативно-правових актів, серед яких необхідно виокремити Конвенцію про кіберзлочинність та Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Аналіз Кримінального кодексу України та ряду інших нормативно-правових актів дозволив зробити висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імплементовані у правове поле нашої держави.

3. Встановлено, що низці кримінальних правопорушень, які передбачені КК України та віднесені до різних його розділів, притаманна загальна характеристика – вчинення з використанням інтернет-банкінгу. На підставі цього, запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь. Охарактеризовано наукові підходи щодо сутності окремих наукових категорій, що характеризують правовідносини у сфері використання банківських електронних платежів, зокрема: «е-банкінг», «електронний бізнес», «цифрова торгівля» та ін.

4. Сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, в якій виокремлено наступні елементи: 1) криміналістична класифікація протиправних діянь; 2) криміналістична характеристика; 3) аналіз початкової інформації щодо вчиненого діяння; 4) обставини, що підлягають встановленню; 5) типові слідчі ситуації та відповідний їм алгоритм дій уповноважених осіб; 6) профілактична діяльність уповноважених осіб зі встановлення причин й умов, що сприяли учиненню кримінальних правопорушень; 7) взаємодія підрозділів правоохоронних органів та інших структур у кримінальному провадженні; 8) початковий етап розслідування; 9) подальший етап розслідування; 10) особливості використання спеціальних знань.

5. Надано авторське визначення криміналістичної характеристики правопорушень, пов’язаних з використанням інтернет-банкінгу, як сукупності даних, отриманих із судово-слідчої практики, про криміналістично значимі ознаки певної категорії протиправних діянь, яка зводиться до кореляційних зв’язків між ними та забезпечує побудову і перевірку криміналістичних версій для вирішення основних завдань кримінального провадження, а також надає додаткову інформацію, необхідну для ефективного проведення слідчих (розшукових) дій та НСРД. На основі вивчення матеріалів кримінальних проваджень визначено перелік основних елементів криміналістичної характеристики правопорушень, пов’язаних із використанням

інтернет-банкінгу.

6. Обґрунтовано, що у переважній більшості випадків (99 %) мають місце повноструктурний склад способу вчинення протиправних дій. Аргументовано, що спосіб є центральним елементом криміналістичної характеристики. В умовах діджиталізації суспільства злочинна діяльність видозмінює свої форми та методи, злочинці дедалі використовують складні й нетипові способи учинення та приховання злочинних дій. На основі вивчення матеріалів кримінальних проваджень охарактеризовано основні підготовчі дії до вчинення кримінальних правопорушень, пов'язаних із 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. Встановлено найбільш типові способи учинення та приховування досліджуваної категорії протиправних діянь.

7. Значну увагу приділено обстановці учинення кримінальних правопорушень як системи об'єктивних чинників й умов матеріальної обстановки, а також просторово-часових характеристик місця та часу. Охарактеризовано місця учинення досліджуваної категорії кримінальних правопорушень. Визначено слідову картину протиправних діянь. Встановлено, що переважний масив слідової інформації залишається у мережі Інтернет (безпосередньо в проведених інтернет-операціях, в кеш-пам'яті або хмарних сховищах). З'ясовано, що у більшості випадків потерпілий не має візуального контакту з правопорушником.

8. Охарактеризовано криміналістично значущі типологічні ознаки особи злочинця та особливості віктимогенної поведінки потерпілих. Надано

перелік ознак і властивостей, що характеризують особу злочинця, зокрема: інтелектуальні, психологічні, соціально-демографічні, моральні та фізичні. Встановлено, що досліджувані протиправні діяння вчинюють переважно чоловіки (91 %). Стосовно критерію віку особи, яка їх вчинила, з'ясовано, що це були особи у віці 16-20 років – 8 %, 20-30 років – 42 %, 30-40 – 26 %, 40-50 років – 19 %, 50 років і старше – 5 %. Відносно рівня освіти правопорушників встановлено наступні дані: базову середню освіту має 1 % правопорушників, середню – 2 %, середню спеціальну – 4 %, базову вищу – 15 %, вищу – 79 %. Підсумовуючи зазначене, було створено ймовірний «портрет» особи правопорушника.

9. Охарактеризовано особу потерпілого. Вирізнено віктимогенні групи осіб щодо яких було вчинено кримінальні правопорушення визначеної категорії: а) працівники фінансових установ, підприємств та організацій різних форм власності; б) їхні клієнти; в) родичі клієнтів. Висвітлено кореляційні зв'язки між елементами криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

РОЗДІЛ 2
ОРГАНІЗАЦІЙНІ ОСНОВИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ

2.1. Криміналістичний аналіз первісної інформації та організація розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу

Аналіз первинної інформації має важливе значення майже у більшості кримінальних проваджень. Стосовно кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, слід зазначити, що вказаний етап дозволяє вирішити питання: а чи взагалі наявний факт скоєння визначеної категорії протиправних діянь? Тому беззаперечно уповноважені особи повинні ретельно і швидко аналізувати всі отримані та наявні відомості будь-якого характеру [134, с. 21].

Стосовно збору початкової інформації велика кількість праць науковців, серед яких ми вважаємо доречним виділити наступних: П. Д. Біленчук, В. І. Перкін [11], В. В. Лисенко [82], О. В. Лускатов [86], О. В. Пчеліна [115], Ю. М. Чорноус [168; 170], В. Ю. Шепітько [175], Б. В. Щур [179] та інші.

Відповідно до ч. 1 ст. 214 КПК України досудове розслідування розпочинається у певний момент, а саме: «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» [75].

Згідно Наказу Генеральної прокуратури № 298 від 30.06.2020, що затверджує «Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення», факт внесення відомостей до Єдиного реєстру досудових розслідувань «…прокурором, слідчим, дізнавачем ще не надає останнім права проводити слідчі (розшукові) та інші процесуальні дії, спрямовані на забезпечення дієвості кримінального провадження і досягнення мети розслідування, оскільки, вказані відомості підлягають перевірці керівником органу прокуратури, органу досудового розслідування, органу дізнання. Факт реєстрації кримінального правопорушення (провадження) настає лише з моменту підтвердження керівником органу прокуратури або органу досудового розслідування, органу дізнання таких відомостей» [110].

Вважаємо за потрібне привести на розгляд позицію В. Г. Дрозд, яка зауважує, що «…досудове розслідування, беззаперечно, є першою та самостійною стадією кримінального процесу України» [31, с. 189]. Повністю поділяємо дане твердження дослідниці, позаяк дійсно до вказаної стадії в КПК нічого не вказується.

В свою чергу, А. Ф. Волобуєв вказує на те, що характер та обсяг інформації про протиправне діяння може бути різним, що залежить, перш за все, від особливостей того чи іншого виду (групи) кримінальних правопорушень. На основі аналізу законодавства та слідчої практики автор визначив наступні підстави для внесення первинного матеріалу в Єдиний реєстр досудових розслідувань: «…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)» [73, с. 11-12].

А вже С. В. Самойлов при дослідженні питань допиту потерпілих від шахрайств, які пов'язані з купівлею/продажем у мережі Інтернет встановив, що переважно джерелами первинної інформації про досліджувані шахрайства становлять: 1) заяви чи повідомлення представника інтернет-сервісу, на якому було виявлено шахрайство – 15%; 2) заяви чи повідомлення від потерпілого – 85%. Крім того, науковець наголосив на тому, що теоретично не можна виключати й інших джерел, найбільш імовірним серед яких можна вважати безпосереднє виявлення ознак кримінального правопорушення працівниками правоохоронних органів: а) під час перевірки одержаної з оперативних джерел інформації про правопорушення, яке вчинено чи готується; б) під час проведення оперативно-розшукових заходів, спрямованих на запобігання злочинам у мережі «Інтернет», у ході яких було виявлено ознаки шахрайства; в) під час досудового розслідування слідчим іншого кримінального правопорушення, якщо під час такого розслідування будуть виявлені обставини, що вказують на шахрайства, вчинені з використанням мережі «Інтернет». Також дослідник на основі опрацьованого емпіричного матеріалу визначив характерні ознаки, наявність яких у первинному матеріалі орієнтує уповноважену особу на викриття ознак

досліджуваного виду шахрайства, зокрема: 1) факт взаємодії потерпілого та зловмисника через мережу «Інтернет»; 2) факт передачі коштів, майна чи права на майно; 3) факт невиконання іншою стороною зобов'язань у межах домовленості [127, с. 82].

Зі свого боку, А. В. Рейнгольд відмічав, 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» [118, с. 22].

Доречною також вважаємо думку С. С. Чернявського, який зробив висновок, що попередня перевірка інформації про кримінальне правопорушення – «…це діяльність уповноважених органів і службових осіб, спрямована на встановлення достовірності інформації, що міститься в первинних матеріалах про злочин, а також збирання додаткових відомостей, що характеризують подію і потрібні для прийняття обґрунтованого рішення про порушення кримінальної справи» [165, с. 16].

На базі вивчення матеріалів кримінальних проваджень [Додаток А] ми підсумували, що первинна інформація, яка була підставою для внесення відомостей до Єдиного реєстру досудових розслідувань за фактом учинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, потрапляли до підрозділів правоохоронних органів наступним чином:

а) заяви, листи та повідомлення від громадян, які є потерпілими від досліджуваних протиправних діянь – 77 %;

б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене протиправне діяння або стали його свідками – 9 %;

в) повідомлення працівників установ, підприємств та організацій – 3 %;

г) матеріали досудового розслідування, виділені з інших кримінальних проваджень – 6 %;

д) матеріали, отримані під час проведення НСРД та розшукових заходів – 5 %.

Підсумовуючи, зазначимо, що аналіз первинної інформації стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, дозволяє вирішити питання наявності в діях правопорушника досліджуваного протиправного діяння.

Однією зі складових методики розслідування окремих кримінальних правопорушень є обставини, які підлягають встановленню. Даний елемент у своїх роботах опрацьовують майже усі науковці, предметом дослідження у яких є вказана тематика. Тому при розгляді розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, ми не могли оминути увагою зазначену складову. Адже вона акумулює в собі загальні відомості стосовно самого протиправного діяння, а також характеристик його учасників, що служить для побудови конкретних слідчих ситуацій в кримінальних провадженнях досліджуваної категорії [137, с. 127].

На початку викладення матеріалу приведемо думку Ю. М. Чорноус, яка наголошує, що «…для кримінального провадження діяльність щодо встановлення обставин конкретного характеру виражається в: фіксації ходу і результатів проведення процесуальних, слідчих (розшукових) дій, негласних слідчих (розшукових) дій; виявленні, фіксації, збиранні, дослідженні слідів злочину; веденні систем кримінальної реєстрації та криміналістичних обліків; залученні спеціальних знань до проведення процесуальних, слідчих (розшукових) дій, негласних слідчих (розшукових) дій; залученні експертів та проведенні судових експертиз та ін.» [169, с. 221].

Окрема група дослідників (О. В. Бишевець, М. А. Погорецький, Д. Б. Сергєєва) вказує на те, що на відміну від термінологічного апарату кримінального процесу, у науці криміналістиці послуговуються дещо іншим

терміном, а саме «обставини, що підлягають встановленню», які відповідно до структури окремих криміналістичних методик, є окремим їх елементом. До обставин, що підлягають встановленню відносяться обставини, що підлягають доказуванню, тобто ті, що становлять предмет доказування, а також проміжні факти й обставини, які необхідно дослідити, але які не входять до предмету доказування, залишаються поза його межами [122, с. 22]

Зокрема, в ст. 91 КПК України визначено перелік обставин, які підлягають доказуванню, а саме: «…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» [75].

В свою чергу, С. М. Стахівський правильно зауважує те, що «…метою

кримінально-процесуального доказування є встановлення об’єктивної істини, а її досягнення можливе лише тоді, коли під час провадження у кримінальній справі з достатньою повнотою і достовірністю будуть встановлені усі факти і обставини, які мають значення для правильного вирішення цієї справи. Сукупність таких фактів і обставин утворюють предмет доказування у кримінальній справі» [147, с. 18].

Доречним вбачаємо позицію К. О. Чаплинського, який поглиблює перспективу опрацювання окремих обставин під час розслідування, а саме: «…виникнення злочинного задуму; відомості про об’єкт посягання, мотив злочину, ставлення особи до злочинних наслідків; способи підготовки та вчинення злочинів, послідовність злочинних дій, а також особливості приховування злочинної діяльності (її характер); час, місце, обстановка та механізм учинення злочинів; відомості про особу злочинця; умови, за яких допитуваний спостерігав будь-які предмети або явища; психологічний та фізичний стан особи в момент сприйняття чи після нього; загальна здібність допитуваного до певного сприйняття, запам’ятовування та відтворення; обставини, що сприяли або перешкоджали учиненню злочинів; способи формування організованої групи та характер злочинної діяльності; виявлення психологічної й функціональної структури групи (якісний склад, рівень організованості) та розподілу функціональних обов’язків; кількісний склад групи при учиненні кожного епізоду злочинної діяльності, конкретні дії кожного, навички володіння зброєю та прийомами боротьби; виявлення осіб, які не брали безпосередньої участі у вчинених злочинах, але обізнаних про їх підготовку, вчинення або приховання; наявність корумпованих зв’язків та зв’язків з іншими злочинними групами; способи протидії розслідуванню та впливу на потерпілих, свідків та членів групи, які дають правдиві показання; наявність в групі конфліктів, протиріч та розбіжностей; способи легалізації отриманих прибутків та відтворення злочинної діяльності; встановлення осіб, які залишилися на волі і продовжують злочинну діяльність або налагоджують зв’язки між членами групи та намагаються створити єдину, вигідну для усіх

лінію поведінки та ін.» [163, с. 210].

Зі свого боку, окрема група науковців (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) визначили наступні обставини, як необхідно доказувати при розслідуванні кримінальних правопорушень у сфері інформаційних технологій, а саме: «1) час вчинення злочину; 2) місце вчинення злочину; 3) особливості і характеристика об'єкта, де вчинено злочин; 4) особливості побудови і організації експлуатації засобів обчислювальної техніки; 5) спосіб злочинного впливу на інформацію (несанкціоноване копіювання; вилучення разом з носієм; перекручення; знищення); 6) характеристика інформації, що зазнала злочинного впливу; 7) засоби, які використовувались при вчинені злочину (технічні засоби; програмні засоби, в тому числі, програми-пастки і комп'ютерні віруси; інші засоби); 8) спосіб подолання програмного і апаратного захисту; 9) можливість вчинення злочину ззовні приміщення через мережі телекомунікації та наявність слідів у вигляді протоколів обміну й іншої комп'ютерної інформації; 10) наявність можливості проникнення на місце злочину і відходу від нього через вікно, двері, пролом, сходи, а також способи відходу (пішки або з використанням транспортного засобу); 11) наявність на об'єкті, шляхах підходу і відходу слідів злочину і злочинця; 12) знаряддя злочину (використане для проникнення на об'єкт і (або) застосоване для розкриття і демонтажу пристроїв обчислювальної техніки), його частини і сліди (їх характеристика, індивідуальні ознаки, спосіб виготовлення, місце придбання, виготовлення, зберігання і можливого використання в минулому); 13) наявність слідів підготовки до вчинення злочину; 14) мета і мотиви вчинення злочину; 15) відомості про особу злочинця; 16) наявність співучасників; 17) ознаки організованої групи; 18) наявність на одязі особи, яка вчинила злочин, при ній або в помешканні слідів і знарядь злочину або його частин; 19) обставини, що сприяли вчиненню злочину [85, с. 474-475].

А вже Т. В. Охрімчук говорячи про розслідування шахрайства з фінансовими ресурсами, вказує на обов'язковість встановлення таких

обставин: «…характеристика діяльності громадянина-підприємця або іншого передбаченого ст. 222 КК України суб'єкта; достовірність та обґрунтованість документів, які були надані кредитно-фінансовим установам, державним органам або іншим кредиторам з метою отримання кредиту, дотації, субсидії, субвенції, пільг щодо оподаткування; рахунки, на які були переказані від кредитора кошти; характер і зміст нормативних актів, положення яких були порушені при вчиненні злочину; осіб, причетних до вчинення злочину; наявність причинного зв'язку між діями винних осіб та їх наслідками; особливості способу вчинення злочину; визначити характер і розмір збитків, завданих кредитору; розмір несплачених податків, загальний розмір заподіяних матеріальних збитків; майно (нерухоме і рухоме), грошові кошти, необхідні для відшкодування завданих збитків; чи є в діях осіб ознаки інших злочинів; обставини, що сприяли вчиненню злочинів» [99, с. 682].

В свою чергу, С. В. Чучко запропонував виділити наступні групи обставини, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет, зокрема: «…1) обставини, що стосуються події шахрайства при купівлі-продажу товарів через мережу Інтернет (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його вартості; розміщення фейкової інформації про продаж товару за умов накладного платежу з подальшим отриманням частини його вартості на платіжну карту (передоплати); створення сайтів магазинів у мережі Інтернет або їх копій, що діють за принципом фірм-одноденок; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати тощо); відомості про знаряддя (засоби) злочину; відомості про сліди злочину; відомості про предмет злочинного посягання (його кількісні та якісні характеристики), тощо); 2) обставини, що стосуються особи потерпілого та злочинця (ознаки суб'єкта злочину: фізична особа, осудність, вік, кваліфікуючі ознаки, які стосуються суб'єкта; кількість

злочинців (наявність розподілу ролей серед шахраїв, функції кожного з них); 3) причинкові обставини: наявність причинного зв'язку між діями винних осіб та їх наслідками; виявлення причин та умов, які сприяли вчиненню злочину; заходи, яких необхідно вжити для їх усунення тощо; 4) решта обставин (вид і розмір шкоди, завданої кримінальним правопорушенням; кваліфікуючі ознаки щодо розміру шкоди завданої злочином; обставини, що обтяжують чи пом'якшують покарання; обставини, що виключають кримінальну відповідальність, чи є підстава для закриття кримінального провадження; обставини, що є підставою для звільнення від кримінальної відповідальності, а також обставини, що виключають факт вчинення підозрюваною особою іншого злочину тощо» [171, с. 96].

Крім того, Б. Є. Лук'янчиков, Є. Д. Лук'янчиков і С. Ю. Петряєв зауважують, коли на початковому етапі розслідування протиправних діянь у сфері інформаційних технологій особа, яка їх вчинила, не встановлена, варто дослідити наступні дані: «…1) про злочини даної категорії, вчинені раніше аналогічним способом в даному та інших районах; 2) про осіб, «які проходять» по цих злочинах; 3) про факти антигромадської поведінки (протиправні способи задоволення потреб) серед осіб: з числа родичів і знайомих потерпілого, які працюють або працювали на об'єкті або їх зв'язки; інших осіб, які опинились на місці злочину, в тому числі, й неповнолітніх; 4) про факти, які вказують на невдоволення деяких осіб з числа працюючих на об'єкті, обстановкою, що там склалася (невизнання наукових, професійних або організаторських здібностей; конфлікти на ґрунті особистої неприязні; невдоволення зарплатою, часом відпустки; затримка з просуванням по службі; інші обставини); 5) про збіг або неспівпадіння відомостей про вищезгаданих осіб з наявними відомостями про особу злочинця; 6) про місце знаходження особи (осіб), яка виявляла зацікавленість, в момент вчинення злочину (причини відсутності за місцем роботи, навчання і вдома). З'ясування даних обставин здійснюється шляхом проведення слідчих (розшукових) дій гласного та негласного характеру» [85, с. 475-476].

Найбільш оптимальною для досліджуваної нами категорії кримінальних проваджень вважаємо систему обставин, яку наводить І. О. Коваленко по розслідуванню шахрайства у сфері використання банківських електронних платежів, а саме: «…1) обставини, котрі характеризують вчинення шахрайства у сфері використання банківських електронних платежів (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, які викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, з персональних комп'ютерів користувачів; відомості про сліди протиправного діяння; визначення місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); засоби, що використовуються при скоєнні правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації); 2) обставини, котрі відносяться до характеристики особи злочинця та особи потерпілого (кількість правопорушників – факт розподілу функцій серед шахраїв, завдання кожного з них); 3) причинно-наслідкові зв'язки: наявність певного зв'язку між діями винних осіб та їх результатами; з'ясування причин та умов, які сприяли вчиненню протиправного діяння; 4) обставини, котрі обтяжують, пом'якшують покарання чи взагалі виключають кримінальну відповідальність (чи наявні умови та підстави для закриття кримінального провадження); 5) кваліфікуючі ознаки стосовно розміру шкоди завданої протиправним діянням та обставини, котрі є підставою для звільнення від кримінальної відповідальності; 6) вид та розмір шкоди, завданої вчиненням шахрайства у сфері використання банківських електронних платежів» [53, с. 100].

З огляду на вищенаведену систему, визначимо перелік обставин, які підлягають встановленню під час розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу:

1) обставини, що характеризують вчинення кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу: а) відомості про час, місце та спосіб учинення протиправних дій, як-от, застосовування шкідливих програм чи вірусів, заведених до комп’ютерного забезпечення потерпілого та дублювання за допомогою них акаунту на власний ґаджет (смартфон, планшет, ноутбук, комп’ютер); б) відомості про віртуальні сліди кримінального правопорушення; в) встановлення місця одержання безпідставного доступу до мережі Інтернет; г) засоби, які застосовувалися під час скоєння протиправного діяння (технічні – різні ґаджети, зокрема, смартфони, ноутбуки, модеми; програмні – шпигунські програми, браузери, шкідливі віруси);

2) обставини, які розкривають особу правопорушника з різних сторін (професійної, злочинної. розумової);

3) обставини, які розкривають особу потерпілого з різних сторін (професійної, злочинної. розумової);

4) причинно-наслідкові взаємозв’язки: факт чіткого зв’язку між діями правопорушників та їх наслідками;

5) обставини, які обтяжують чи пом’якшують покарання, або у цілому виключають кримінальну відповідальність за скоєння протиправних діянь, пов’язаних із використанням інтернет-банкінгу.

Підводячи підсумок, зазначимо, що обставини, які підлягають встановленню під час розслідування кримінальних правопорушень, пов’язаних з використанням інтернет-банкінгу, акумулюють в собі загальні відомості стосовно самого протиправного діяння, а також характеристик його учасників, що служить для побудови конкретних слідчих ситуацій в кримінальних провадженнях досліджуваної категорії. Визначено перелік обставин, які підлягають встановленню під час розслідування досліджуваної

категорії протиправних діянь.

В розрізі зазначеного вважаємо необхідним звернутися до визначення запобіжних заходів, які необхідно здійснювати для попередження вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

З приводу профілактичних заходів за останні роки було досить багато досліджень серед науковців, серед яких ми вважаємо за доцільне вирізнити таких як О. А. Антонюк [3], А. Ф. Волобуєв [19], Н. І. Головко [21], В. Г. Дрозд [28], М. М. Єфімов, К. О. Чаплинський [36], В. М. Тертишник [153], В. Ю. Шепітько [176] та інші.

Відносно предмету криміналістичної профілактики вважаємо найбільш точним перелік, наведений С. В. Томіним, як-от: «…закономірності утворення, виявлення та дослідження слідів прояву криміногенних обставин під час підготовки, вчинення і приховання окремих видів і категорій злочинів відомими криміналістам способами (незалежно від того, чи застосовувались такі способи злочинцями, чи застосування їх є можливим і прогнозується криміналістами); техніко-криміналістичні засоби захисту об'єктів від злочинних посягань, що сприяють виявленню і припиненню злочинів, а також використовуються з метою отримання, накопичення і видачі інформації про знаряддя і засоби, що використовуються під час вчинення злочинів, та осіб, схильних до їх вчинення; техніко-криміналістичні засоби, прийоми і методи виявлення, фіксації і дослідження криміногенних обставин; тактичні прийоми і засоби найбільш ефективного виявлення і усунення криміногенних обставин, а також запобігання і припинення злочинів; криміналістичні методи або системи прийомів виявлення і усунення причин і умов вчинення злочинів, а також припинення і попередження злочинів [157, с. 124].

Також з приводу формулювання визначення профілактики кримінальних правопорушень ми підтримуємо позицію А. Е. Жиліна. Зокрема, автор сформулював вказану наукову категорію наступним чином: «…це система конкретних дій (заходів), які здійснюють уповноважені особи

правоохоронних органів (дізнавачі, слідчі, прокурори та інші), що мають на меті усунення причин та умов вчинення протиправних діянь конкретної категорії» [37, с. 145].

Стосовно профілактичної функції працівників правоохоронних органів ми підтримуємо позицію М. М. Єфімова та Є. А. Омарова, які зауважують, що вона обов'язково повинна реалізуватися незалежно від служби, де працює той чи інший правоохоронець, та від його посади. Також дослідники наголошують, що раніше КПК України прямо зобов'язував уповноважених осіб реалізовувати ряд заходів відносно усунення причин та умов вчинення кримінальних правопорушень. Крім того, автори підмічають, що на даний час така норма відсутня. Наостанок науковці зробили висновок, що уповноважені особи, які виконують досудове розслідування (слідчий, дізнавач, прокурор) зобов'язані відшукувати всі можливі способи, щоб зробити хоча б щонайменше для запобігання вчинення кримінальних правопорушень [189, с. 114].

Найбільш широкий перелік заходів з профілактики комерційних інтернет-шахрайств, на нашу думку, надав у власному дисертаційному дослідженні А. В. Рейнгольд. Автор серед них виокремив такі як: «…розміщення оголошень в ЗМІ щодо способів комерційних інтернет-шахрайств та заходів їх запобігання; виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу; відслідковування операцій, які потенційно можуть бути шахрайськими з урахуванням кількості карток клієнта, його місцезнаходженням та місцем здійснення операції, місцезнаходженням та адресою доставки, тощо; використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства; актуалізація законодавчих актів, що регулюють інтернет-відносини; підсилення відповідальності за вчинення шахрайств у мережі Інтернет; посилення відповідальності адміністраторів баз даних та інших осіб, які забезпечують функціонування мережі Інтернет, електронних вузлів та пристроїв; підсилення міжнародного співробітництва у

боротьбі із комерційним кібершахрайством; створення Єдиної інформаційної системи, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв, які вчиняють комерційні інтернет-шахрайства; залучення громадськості з профілактики шахрайства в сфері електронної торгівлі» [117, с. 149].

Запропоновано систему запобіжних заходів, котрі необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні досліджуваної категорії протиправних діянь, а саме:

1) застосовування протоколів безпеки, зокрема, використання криптографічних функцій, а також системи аутентифікації користувачів шляхом перевірки правильності внесених даних і запобігання заміни особи;

2) застосовування технологій фіксації транзакцій, для прикладу, блокчейн, що допускають фіксувати всю інформацію;

3) повідомлення громадян через ЗМІ, соціальні мережі та месенджери (Viber, Telegram, WhatsApp) про факти скоєння кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу (фішинг, кардинг);

4) встановлення осіб, які мають нахили до антисуспільної поведінки в інформаційній сфері та постановка їх на відповідні обліки у підрозділах правоохоронних органів (зокрема, кіберполіції).

Підсумовуючи, відмітимо, що запобіжні заходи, які необхідно здійснювати для попередження вчинення кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, є важливим аспектом кримінальних проваджень визначеної категорії.

2.2. Типові слідчі ситуації, що виникають під час розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу

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 із 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 із використанням інтернет-банкінгу [139, с. 129].

З приводу типових слідчих ситуацій одразу вважаємо за доцільне звернутися до дослідження С. В. Веліканова, який ще на початку 2000-х зауважував, що органам розслідування доводиться діяти в різних умовах і обставинах, які складаються під впливом особливостей протиправних діянь, дефіциту часу та доказової інформації, специфіки відносин між учасниками кримінального процесу. Також автор акцентував увагу на тому, що у такому аспекті процес розслідування вбачається як система слідчих ситуацій, які змінюються протягом усього періоду кримінального провадження. Крім того, науковець зазначав, що виділення слідчої ситуації об’єктом власного наукового дослідження зумовлюється потребою виявлення особливостей криміналістичного підходу до вивчення процесу досудового слідства як стадії кримінального судочинства. На останок, вчений-криміналіст сформулював наступне визначення окресленої наукової категорії: «…це сукупність сформованих на певному етапі умов – положення, стану й обстановки – розслідування, що сприймаються, оцінюються і використовуються слідчим для вирішення тактичних задач і досягнення загальних (стратегічних) цілей розслідування» [13, с. 1, 7]. Як бачимо, питання типових слідчих ситуацій було актуальним ще на початку сторіччя і з часом не втратило свого значення.

Досить точно Є. С. Хижняк свідчить про те, що вказана наукова категорія (як і криміналістична характеристика) є одним із найбільш

важливих інструментів у руках уповноваженої особи, яка здійснює доказування. Автор наголошує, що вказане дає змогу максимально підвищити ефективність діяльності з розслідування протиправних діянь, а володіння типовими слідчими ситуаціями дає змогу уповноваженій особі окреслити коло пріоритетних завдань, а також уникнути непотрібної витрати часу та сил. Крім того, дослідник зауважує, що «…на основі зіставлення типової слідчої ситуації й ситуації, що сталася під час розслідування конкретного злочину, використовуючи взаємозв'язки між елементами криміналістичної характеристики цієї групи злочинів, слідчий зможе оптимально спланувати процес розслідування та найефективніше вирішити завдання встановлення особи, яка вчинила злочин» [159, с. 197].

Відносно самостійності слідчого В. Г. Дрозд зауважувала, що вона «…полягає в його можливості, як учасника кримінального провадження, здійснювати досудове розслідування без стороннього впливу будь-яких інших фізичних чи юридичних осіб, службових осіб, представників державної влади чи місцевого самоврядування» [29, с. 33].

Також вважаємо вірною думку В. Ю. Шепітька, який зауважував наступне: «Аналогічність, типовість слідчих ситуацій і відповідно шляхів, що ведуть до їх вирішення, дозволяють говорити про можливість програмування (алгоритмізації) дій слідчого. Важливим для створення ефективних програм розкриття і розслідування злочинів є метод узагальнення ситуацій — так зване ситуаційне моделювання, яке дає змогу розробляти оптимальні програми прийняття рішень і проведення тактичних комплексів (застосування тактичних операцій) та окремих слідчих дій» [72, с. 283].

А вже А. Ф. Волобуєв наголошував на тому, що «Типові, тобто найбільш характерні слідчі ситуації відіграють ключову роль у формуванні практичних рекомендацій у кожній окремій методиці розслідування. Під слідчою ситуацією в криміналістиці розуміють умови розслідування злочину на певний його момент. Серед умов розслідування виділяють такі: – інформаційні фактори (відомості про злочин – докази, оперативно-розшукова

інформація); – процесуальні фактори (наприклад, наявність підозрюваного на певний момент розслідування); – тактичні фактори (наприклад, позиція, яку займає підозрюваний на допиті); – психологічні фактори (психологічні особливості осіб, що беруть участь у розслідуванні); – матеріально-технічні й організаційні фактори (наявність необхідних засобів і можливостей їх використання). Це – поняття слідчої ситуації в широкому її розумінні. Але під час побудови окремих методик розслідування виявилося, що дуже важко типізувати деякі фактори, наприклад психологічні, матеріально-технічні й організаційні. Тому в криміналістичній методиці використовується поняття слідчої ситуації у вузькому розумінні – як сукупності відомостей про злочин, яка обумовлює завдання розслідування й відповідні засоби їх вирішення – гласні та негласні слідчі (розшукові) дії. Типові слідчі ситуації формуються в окремих методиках розслідування вже на стадії відкриття кримінального провадження залежно від характеру первинного матеріалу про злочин» [73, с. 12].

В свою чергу, М. М. Єфімов вказував на те, що «…у ході розслідування слідчий ознайомлюється з великою кількістю речових доказів, документів. Автор зазначає, що означена уповноважена особа реалізує це з метою безпосереднього отримання інформації в результаті проведення оперативно-розшукових і слідчих (розшукових) дій. Враховуючи це, приймаються відповідні рішення про організацію та планування процесу розслідування злочинів, використання допомоги спеціалістів й інших підрозділів органів внутрішніх справ. Дані про обставини вчинення злочину є предметом аналізу у процесі розслідування. Сукупність зазначеної інформації, отриманої з різних джерел, становить зміст слідчої ситуації» [35, с. 145].

Зі свого боку, С. С. Чернявський формулює типову слідчу ситуацію як інформаційну модель з найбільш значущими властивостями та ознаками процесу розслідування в кримінальних провадженнях щодо злочинів певної категорії [166, с. 405].

Також вважаємо доречною позицію А. Іщенка та Г. Щербакова, які акцентували увагу на тому, що вивчення питання слідчої ситуації як криміналістичної категорії має теоретичне та прикладне значення. Крім того, автори зазначили, що теоретичне значення розроблення цієї проблеми в загальному полягає в об'єктивній необхідності конкретизації змісту та поняття вказаної наукової категорії. З приводу його практичного значення дослідники зауважили, що воно полягає в тому, що визначення змісту слідчих ситуацій, їх класифікація, аналіз і оцінка дають можливість об'єктивно обґрунтувати вибір варіантів методики розслідування, які найбільшою мірою відповідали б обставинам і завданням розслідування на певному етапі [48, с. 57].

А вже Р. Л. Степанюк засвідчував, що досліджувана наукова категорія може бути визначена наступним чином: «…сформульована на підставі аналізу практики розслідування певної категорії злочинів абстрагована штучна модель, яка відображає стан наявної у слідчого інформації про обставини злочину й обставини, що склалися на відповідному етапі розслідування» [150, с. 111].

Цікавим вважаємо твердження С. В. Веліканова з приводу того, що вивчення природи та структури слідчої ситуації дозволяє зробити вивід про сутність досліджуваного явища. Серед аспектів, які характеризують наведене, науковець виокремив такі: «…1) криміналістична сутність слідчих ситуацій виявляється в специфіці обстановки і стану розслідування в процесі їх формування, розвитку і вирішення; 2) соціолого-правовий аспект полягає в тому, що слідча ситуація розвивається і складається в рамках, установлених чинним законодавством (матеріальним і процесуальним) при відповідному рівні сформованих відносин; 3) інформаційно-психологічний аспект полягає в тому, що всяка ситуація представляється у вигляді сприйнятої слідчим сукупності даних, що характеризують стан і обстановку розслідування, використовуваних для оцінки і моделювання як слідчих ситуацій, так і засобів їх вирішення відповідними методами» [14, с. 33].

Підсумовуючи, сформулюємо авторське визначення типової слідчої ситуації – це побудована на основі опрацювання певної категорії кримінальних проваджень інформаційна модель з найбільш значимими ознаками та властивостями окремої категорії кримінальних правопорушень.

З приводу класифікації типових слідчих ситуацій, то переважна більшість науковців, як вірно вказує В. М. Шевчук, вводять за основу в першу чергу критерій складності: прості та складні. Також автор зауважує, що при цьому слідча ситуація є складною і в тих випадках, коли реальна інформаційна невизначеність вимагає побудови декількох її імовірнісних моделей. На основі вищезазначеного науковець зробив наступний висновок: «Якщо ж інформації про ситуацію достатньо для побудови її однозначної моделі, то така ситуація буде простою. В основі поділу лежить характеристика одного з компонентів інформаційного характеру – проінформованості слідчого» [174, с. 143].

В свою чергу, В. К. Весельський зазначає, що «…в основі всіх загальноприйнятих у криміналістиці класифікацій лежить якась одна ознака. Підставою ж для загальної класифікації слідчих ситуацій є її якісна, стосовно можливості досягнення цілей розслідування, характеристика. Тому він поділяє всі слідчі ситуації на сприятливі та несприятливі для розслідування і вважає, що досягнення слідчим будь-якої з намічених цілей має починатися з оцінки наявної слідчої ситуації й, за необхідності, – з ужиття заходів щодо зміни її в сприятливу сторону» [15, с. 195].

Стосовно класифікацій типових слідчих ситуацій при розслідуванні кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, наведемо позиції дослідників, які опрацьовували дотичні тематики. Наприклад, І. О. Коваленко на початковому етапі розслідування шахрайства у сфері використання банківських електронних платежів виокремив наступні ситуації: «…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 %» [57, 110].

Зі свого боку, окрема група науковців (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв), залежно від характеру та обсягу отриманої інформації, на початковому етапі розслідування кримінальних правопорушень у сфері інформаційних технологій виділяє наступні ситуації: «…1) є відомості про факти незаконного втручання в роботу ЕОМ та їхню систему (перекручування чи знищення комп'ютерної інформації та її носіїв), при цьому відомості про спосіб доступу до неї і осіб, що вчинили дане діяння, відсутні; 2) встановлені факти злочинного заволодіння комп'ютерною інформацією, при цьому відомості про спосіб доступу до неї і осіб, що вчинили дане діяння відсутні; 3) встановлені порушення правил експлуатації ЕОМ та їхніх систем (крадіжка, перекручування, копіювання, істотне порушення роботи ЕОМ), при цьому відомості про осіб, що вчинили дане діяння, відсутні; 4) встановлені факти злочинного впливу на комп'ютерну інформацію (заволодіння, перекручення або руйнування), при цьому є відомості про спосіб доступу і осіб, що вчинили дане діяння» [85, с. 473].

Стосовно визначення слідчої ситуації та її особливостей під час розслідування протиправних діянь у сфері інформаційних комп'ютерних технологій, то О. І. Мотлях вказав, що «…це пізнана суб'єктом доказування об'єктивна реальність (матеріальні та ідеальні джерела), яка існує на даний момент розслідування злочину. Показано, що формування слідчої ситуації у злочинах з використанням інформаційних комп'ютерних технологій відбувається під впливом об'єктивних та суб'єктивних факторів. З метою більш доступного сприйняття слідчим та іншими учасниками процесу

нетрадиційних видів злочину, автором сформульовано та запропоновано кілька типових слідчих ситуацій, що можуть скластися при розслідуванні справ, пов'язаних з комп'ютерними технологіями залежно від впливу на комп'ютерну інформацію» [93, с. 10-11].

Цікавою також є позиція Д. В. Пашнєв та М. Г. Щербаковського, які стосовно кримінальних проваджень за ст. 361–363-1 КК України, зазначають, що вони можуть бути відкриті за зверненням (заявою) власника комп'ютерної інформації (юридичної або фізичної особи) або в результаті виявлення ознак протиправного правоохоронним органом. А вже залежно від характеру вихідних даних про ознаки кримінального правопорушення науковці виділяють такі типові слідчі ситуації початкового етапу розслідування: «…Ситуація 1. Кримінальне провадження відкрито за зверненням (матеріалами) заявника, в якому встановлено ознаки злочину, вчиненого невідомою особою. Ситуація 2. Кримінальне провадження відкрито за зверненням (матеріалами) заявника, в якому зафіксовано ознаки злочину, вчиненого встановленою особою. Ситуація 3. Кримінальне провадження відкрито в результаті виявлення ознак злочину правоохоронним органом у процесі розслідування іншого злочину» [73, с. 265-266].

В свою чергу, С. В. Самойлов відносно шахрайства, що вчиняється з використанням мережі «Інтернет», вирізняв наступні типові слідчі ситуації початкового етапу розслідування: «…1) виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця або встановлено, або достатньо даних для її встановлення; 2) виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено, однак є певні відомості, що можуть вказувати на неї; 3) виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї» [128, с. 9].

Доречною також вважаємо думку О. Ю. Довженка, який відмічає, що «…типова слідча ситуація на початковому етапі розслідування кіберзлочинів

характеризується, зазвичай, як виявлення ознак злочину, що відбувається одразу після його скоєння, або через певний час. Показується, що з урахуванням особливостей кіберзлочину, здійснення більшості невідкладних слідчих дій, що передбачені процесуальним законом для звичайних злочинів, уявляється неможливим, через фізичну відсутність злочинця в місці настання злочинного результату та здійснення злочинного впливу на відстані» [25, с. 114].

А вже А. І. Кунтій вказував, що на початковому етапі розслідування кримінальних правопорушень в сфері ЕОМ можуть виникнути наступні типові слідчі ситуації: «…1) установлений факт неправомірного доступу до комп'ютерної інформації, є сліди злочину, встановлена особа злочинця, яка не заперечує своєї вини; 2) встановлений факт неправомірного доступу до комп'ютерної інформації, є сліди, що прямо вказують на особу злочинця, але він заперечує свою причетність до вчинення злочину; 3) установлений факт неправомірного доступу до комп'ютерної інформації, відомі особи, які за своїм службовим становищем несуть за це відповідальність, але характер їх особистої провини, а також обставини доступу є невідомими; 4) встановлений факт неправомірного доступу до інформації, вчинити який та скористатися результатами могли тільки особи з певного кола або відомі особи (фірми чи організації), зацікавлені в отриманні цієї інформації, однак недостатньо доказів, що свідчать про їх причетність, невідомий механізм учинення злочину; 5) коли є злочинний результат, наприклад дезорганізація комп'ютерної мережі банку, проте механізм злочину та злочинець невідомі» [71, с. 877].

На останок приведемо позицію С. В. Чучка, який на основі аналізу судово-слідчої практики сформулював типові слідчі ситуації розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет, а саме: «…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 %» [172, с. 128].

На основі вивчення слідчо-судової практики [Додаток А] нами було визначено наступні типові слідчі ситуації початкового етапу розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, а саме:

1) скоєно кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, має місце достатня доказова база, особу правопорушника встановлено – 6 %;

2) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника не встановлено – 64 %;

3) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника встановлено, та протиправні дії приховані під легальну фінансову діяльність – 9 %;

4) скоєно протиправне діяння, має місце заява потерпілого, відсутня будь-яка доказова база – 21 %.

Крім того було представлено алгоритми вирішення кожної з них. Для прикладу, *у першій ситуації* (наявна особистісна доказова інформація та правопорушник відомий) уповноважена особа повинна провести комплекс заходів, за допомогою яких необхідно з'ясувати можливі обставин провадження для доказування вини правопорушника, зокрема: огляд засобів електронно-обчислювальної техніки правопорушника під час проведення обшуку (смартфонів, планшетів, ноутбуків, персональних комп'ютерів); допит підозрюваного з приводу обставин обману громадян та законності його діяльності; допит потерпілого щодо обставин зняття коштів через інтернет-банкінг; затребування відомостей від інтернет-провайдерів та

операторів телекомунікаційного зв'язку; з'ясування умов створення фіктивного сайту, створення програм віддаленого доступу, «троянів», «ботів»; пред'явлення підозрюваного для впізнання потерпілому за голосом (у разі спілкування в телефонному режимі) та в натурі (у разі комунікації у режимі відео-конференції); призначення комп'ютерно-технічної та інших видів експертиз.

Друга ситуація є найбільш розповсюдженою у досліджуваній категорії кримінальних проваджень – наявна особистісна доказова інформація, але правопорушник невідомий. Для її вирішення всі зусилля уповноважених осіб повинні бути направлені на встановлення особи, яка вчинила кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, а також її місцезнаходження. Для реалізації вказаного потрібно проводити комплекс розшукових заходів, спрямованих на встановлення IP-адреси та осіб, які мали доступ до електронно-обчислювальної техніки.

У *третій ситуації* (наявна матеріальна та особистісна доказова інформація, правопорушник відомий, але його дії замасковані під вид законних фінансових операцій) уповноважені особи повинні спрямувати усі зусилля на опрацювання змісту файлів й аналізу змісту web-браузерів, а також дослідження змісту електронної пошти, журналу вхідних і вихідних дзвінків на усіх доступних ґаджетах потерпілого.

Вказана ситуація корелюється з вказаною в своїй роботі Г. В. Захаровою, яка зазначала, що у випадках, «…коли особи шахраї не переховуються від правоохоронних органів, але свою причетність до вчинення шахрайства заперечують, перед слідчим постають завдання щодо необхідності виявлення, зібрання, та отримання певної сукупності, належних, обґрунтованих, та достатніх обвинувальних доказів, шляхом з'ясування у потерпілих осіб всіх обставин, за яких розпочиналися та завершилися шахрайські дії, і роль кожної причетної (підозрюваної) до цього особи, здійснення детального огляду місця події, вилучення слідів, які вказують на факт шахрайства. Встановлення можливих його свідків. Проведення

впізнання осіб причетних до шахрайських дій, термінове проведення обшуків житла та іншого їх володіння, з метою вилучення електронних носіїв, та інших документів і предметів, які свідчать про вчинення шахрайських дій. Для покращення результативності розслідування доцільно проводити й негласні слідчі (розшукові) дії з метою встановлення злочинних зв'язків шахрая, його образу життя, можливого місця знаходження, речей предметів, документів, що підтверджують причетність до шахрайства та інших доказів, які цікавлять слідство» [43, с. 114].

Четверта ситуація (наявна заява від потерпілого та відсутня достатня доказова інформація) вирішується завдяки проведенню максимальної кількості СРД, НСРД та інших розшукових заходів для з'ясування як обставин учиненого протиправного діяння, так і встановлення особи правопорушника.

В свою чергу, Д. В. Пашнєв та М. Г. Щербаковський вказують на наявність наступних тактичних завдань. Зокрема, дослідники наголосили на обов'язковому встановленні наступних фактів: місця неправомірного проникнення в комп'ютерну мережу (зсередини організації або ззовні); способу здійснення неправомірного доступу (копіювання, модифікація, знищення інформації, внесення шкідливих програм) і його результати; засобів, що були використані для вчинення злочину (технічні, програмні, носії інформації); способів подолання захисту (підбір ключів і паролів, викрадання паролів, відключення засобів захисту тощо); виявлення слідів протиправного діяння. Крім того, автори зауважили, що для реалізації названих завдань повинні бути здійснені наступні першочергові слідчі (розшукові) дії: «…огляд місця події (якщо це не було здійснено до початку кримінального провадження), допит свідків (персоналу організації, де виявлено правопорушення) та потерпілого, призначення комп'ютерно-технічної експертизи. Потім ухвалюються процесуальні рішення щодо тимчасового доступу до документів і заходів щодо встановлення та розшуку винного, пошуку його робочого місця, звідки

відбувалось вторгнення в комп'ютер (комп'ютерну систему). Здійснюється перевірка за криміналістичними обліками з метою одержання даних, які дозволяють зробити висновки (висунути версії) про причетність певної особи до вчиненого злочину, скоєнню декількох злочинів в один спосіб та ін. На цій підставі можуть бути проведені негласні слідчі (розшукові) дії (аудіо-, відеоконтроль особи – ст. 260 КПК України, арешт, огляд і виїмка кореспонденції – ст. 261-262 КПК України, зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем – ст. 263-264 КПК України, спостереження за особою, річчю або місцем – ст. 269 КПК України, аудіо-, відеоконтроль місця – ст. 270 КПК України та ін.» [73, с. 264-265].

Також для вирішення вказаних слідчих ситуацій запропоновано вирішення наступних тактичних завдань:

1) з'ясування механізму кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу;

2) визначення точок доступу, з яких реалізувалися протиправні дії;

3) перевірка цифрових слідів, які залишені під час проведення електронних операцій;

4) встановлення осіб, які реалізували незаконне втручання в роботу інтернет-банкінгу;

5) перевірка мобільних контактів правопорушника та його особистих зв'язків;

6) перевірка банківських і поштових переказів правопорушника;

7) з'ясування всіх епізодів протиправної діяльності; 8) вжиття заходів стосовно попередження протидії розслідуванню.

Підводячи підсумок, зазначимо, що типові слідчі ситуації є одним із найбільш важливих інструментів у руках уповноваженої особи для раціонального спрямування розслідування кримінальних правопорушень. Надано авторське визначення як побудованої на основі опрацювання певної категорії кримінальних проваджень інформаційної моделі з найбільш

значимими ознаками та властивостями окремої категорії кримінальних правопорушень. На основі вивчення слідчо-судової практики було визначено наступні типові слідчі ситуації початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу.

Висновки до розділу 2

Під час аналізу проблемних питань організаційних основ розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, було зроблено наступні висновки:

1. Охарактеризовано правові підстави початку кримінального провадження та визначено обставини, які підлягають встановленню. З’ясовано, що первинна інформація, яка була підставою для внесення відомостей до ЄРДР за фактом учинення кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, надавалася до підрозділів правоохоронних органів наступним чином: а) заяви, листи та повідомлення від громадян, які є потерпілими від досліджуваних протиправних діянь – 77 %; б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене протиправне діяння або стали його свідками – 9 %; в) повідомлення працівників установ, підприємств та організацій – 3 %; г) матеріали досудового розслідування, виділені з інших кримінальних проваджень – 6 %; д) матеріали, отримані під час проведення НСРД та розшукових заходів – 5 %.

2. На підставі узагальнення матеріалів кримінальних проваджень визначено джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт учинення протиправних дій в кіберпросторі.

3. З’ясовано коло обставин, що підлягають встановленню, зокрема:

а) відомості про час, місце та спосіб учинення протиправних дій, як-от, застосовування шкідливих програм чи вірусів, заведених до комп'ютерного забезпечення потерпілого та дублювання за допомогою них акаунту на власний ґаджет (смартфон, планшет, ноутбук, комп'ютер); б) відомості про віртуальні сліди кримінального правопорушення; в) встановлення місця одержання безпідставного доступу до мережі Інтернет; г) засоби, які застосовувалися під час скоєння протиправного діяння (технічні – різні ґаджети, зокрема, смартфони, ноутбуки, модеми; програмні – шпигунські програми, браузери, шкідливі віруси); 2) обставини, які розкривають особу правопорушника з різних сторін (професійної, злочинної. розумової); 3) обставини, які розкривають особу потерпілого з різних сторін (професійної, злочинної. розумової); 4) причинно-наслідкові взаємозв'язки: факт чіткого зв'язку між діями правопорушників та їх наслідками; 5) обставини, які обтяжують чи пом'якшують покарання, або у цілому виключають кримінальну відповідальність за скоєння протиправних діянь, пов'язаних із використанням інтернет-банкінгу.

4. Запропоновано систему запобіжних заходів, котрі необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні досліджуваної категорії протиправних діянь, зокрема: 1) застосовування протоколів безпеки, зокрема, використання криптографічних функцій, а також системи аутентифікації користувачів шляхом перевірки правильності внесених даних і запобігання заміни особи; 2) застосовування технологій фіксації транзакцій, для прикладу, блокчейн, що допускають фіксувати всю інформацію; 3) повідомлення громадян через ЗМІ, соціальні мережі та месенджери (Viber, Telegram, WhatsApp) про факти скоєння кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу (фішинг, кардинг); 4) встановлення осіб, які мають нахили до антисуспільної поведінки в інформаційній сфері та постановка їх на відповідні обліки у підрозділах правоохоронних органів (зокрема, кіберполіції).

5. Здійснено аналіз наукових розробок учених стосовно поняття, сутності та видів слідчих ситуацій.

6. Сформульовано типові слідчі ситуації розслідування кримінальних правопорушень та визначено алгоритми дій правоохоронних органів відповідно до кожної з них.

7. Сформульовано відповідні тактичні завдання, що необхідно вирішувати у кримінальних провадженнях досліджуваної категорії: 1) з'ясування механізму кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу; 2) визначення точок доступу, з яких реалізувалися протиправні дії; 3) перевірка цифрових слідів, які залишені під час проведення електронних операцій; 4) встановлення осіб, які реалізували незаконне втручання в роботу інтернет-банкінгу; 5) перевірка мобільних контактів правопорушника та його особистих зв'язків; 6) перевірка банківських і поштових переказів правопорушника; 7) з'ясування всіх епізодів протиправної діяльності; 8) вжиття заходів стосовно попередження протидії розслідуванню.

РОЗДІЛ 3
ТАКТИКА ПРОВЕДЕННЯ ОКРЕМИХ ПРОЦЕСУАЛЬНИХ ДІЙ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ

3.1. Початковий етап розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу

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 із 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. Вказане потребує відповідного опрацювання та викладення [187, с. 112].

Починаючи розгляд початкового етапу розслідування звернемося до дисертаційного дослідження С. В. Веліканова, який в ньому зауважував наступне: «Елемент «етап розслідування» як компонент просторово-часової локалізації може приймати такі значення: «первинний», «наступний», «завершальний»; елемент «професійні якості особи, що здійснює розслідування» – «висококомпетентна», «компетентна», «недостатньо компетентна», «некомпетентна» і ін.; елемент «наслідки злочину» –

складений, і в залежності від виду розслідуваного злочину змінює свою структуру, включаючи різні лінгвістичні перемінні, наприклад, при розслідуванні корисливих злочинів така його частина, як лінгвістична перемінна «заподіяний збиток», приймає наступні значення: «значний», «великий», «особливо великий». Таким чином, у залежності від ситуації, лінгвістичні перемінні приймають відповідні значення. Набір таких значень у кожному конкретному випадку індивідуальний» [14, с. 50-51]. А вже О. С. Саінчин виокремлює початковий, наступний та завершальний етапи розслідування. Крім того, автор вказує, що початковий етап розслідування починається з моменту знаходження ознак вчинення кримінального правопорушення. Також науковець зазначає, що вказаний етап триває до моменту встановлення особи, підозрюваної у вчиненні протиправних діянь, і визначення ступеня її вини вирішується питання про повідомлення про підозру [123]. Як бачимо, різні дослідники по неоднаково визначають назви етапів «первинний»-«початковий». Але різниця в назві не змінює їх змістовне наповнення. Ми в своїй роботі вирішили вживати терміни «початковий» та подальший» етапи розслідування.

Говорячи про початковий етап кримінального провадження вважаємо привести позицію В. В. Тіщенка, який вказував на такі завдання, які під час нього реалізуються, а саме: «1. Виявлення і фіксація доказової інформації щодо злочину, який розслідується по «гарячих слідах». 2. Вжиття заходів для запобігання втраті доказової інформації, що міститься в слідах, документах, інших об’єктах, її своєчасне виявлення та фіксація. 3. З’ясування й оцінка сформованої після порушення кримінальної справи слідчої ситуації. 4. Виявлення джерел інформації про розслідуваний злочин. 5. Визначення напряму розслідування і розробка плану розслідування. 6. Обрання форми і методів взаємодії з органами і службами, що здійснюють оперативно-розшукову роботу. 7. Пошук і одержання інформації про механізм і обстановку вчиненого злочину. 8. Збирання і вивчення відомостей про особистість потерпілого. 9. Пошук, одержання й аналіз інформації про осіб,

що вчинили злочин, їхній розшук і затримання» [155, с. 137].

В свою чергу, О. М. Дуфенюк вказує на те, що початковий етап розслідування передбачає «…збирання та оцінювання первинної інформації, встановлення наявності чи відсутності ознак кримінального правопорушення у діянні особи (осіб) чи в події (факті), яка сталася; ухвалення рішення про внесення відомостей до ЄРДР та початку досудового розслідування; проведення невідкладних слідчих (розшукових) дій; вжиття заходів щодо розкриття кримінального правопорушення по «гарячих слідах»; визначення напрямів розслідування; формулювання первинних версій. На початковому етапі можемо констатувати про існування дослідчої ситуації, яка й визначатиме послідовність проведення тих чи інших процесуальних дій, ухвалення процесуальних рішень, вжиття інших заходів. Криміналістична ситуація, яка є до початку кримінального провадження, має зазвичай незначний обсяг доказової інформації. Тож основним завданням початкового етапу досудового розслідування є інтенсивний процес збирання (виявлення, фіксації, вилучення, зберігання) доказів» [71, с. 511-512].

Інша група науковців (О. В. Узунова, К. В. Калюга) на базі власного дослідження зробили висновок, що «…початковий етап розслідування характеризується невизначеністю, пов’язаною з браком інформації та її неповнотою, тому домінуючим напрямом діяльності слідчого на цьому етапі є «виявлення необхідної доказової і тактичної інформації та її носіїв (джерел). Це завдання вирішується з урахуванням слідчої ситуації, що складається, шляхом проведення комплексу слідчих, інших процесуальних і організаційних дій. Найчастіше підставою для провадження слідчих дій є криміналістична версія. Основним завданням початкового етапу, як правило, є встановлення особи, причетної до вчинення злочину. Тому збирання інформації про неї розпочинається з ретроспективного вивчення слідів, залишених на місці злочину, у пам’яті очевидців, тощо. Отримана інформація використовується для висунення версій про суб’єкта злочину, визначення напряму його пошуку» [158]. Виходячи з вищенаведених тверджень, можемо

зробити висновок, що початковий етап акумулює процесуальні дії, необхідні для максимального збору доказової інформації на початку кримінального провадження.

Стосовно початкового етапу розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, то, наприклад, окрема група науковців (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) зазначає, що повідомлення про несанкціоноване проникнення в комп'ютерну систему чи комп'ютерну мережу частіше надходить від користувачів, котрі виявили подібний факт. Автори наголошують, що це буває у випадках, коли комп'ютер починає повідомляти фальшиві дані, часто відбуваються збої, знищується частина або вся корисна інформація, надходять скарги клієнтів комп'ютерної мережі. Крім того, науковці акцентують увагу на тому, що це може бути ознаками протиправних дій: неправомірного проникнення чи застосування шкідливих програм або порушення правил експлуатації. Також вчені-криміналісти вказують на наступні можливість висунення та опрацювання таких типових версій початкового етапу розслідування як «…1) комп'ютерний злочин вчинений з метою отримання матеріальної вигоди: а) співробітником даної установи, що володіє навичками роботи з комп'ютерною технікою; б) групою осіб за попередньою змовою або організованою групою за участю співробітника даної установи; в) групою осіб без участі співробітників даної установи, один із злочинців володіє навичками роботи з комп'ютерною технікою; 2) злочин вчинено з метою заволодіння інформацією з обмеженим доступом: а) особою (особами), що має вільний доступ до комп'ютерної техніки; б) особою (особами), що не має вільного доступу до комп'ютерної техніки; 3) злочин вчинено з метою підготовки до розкрадання матеріальних цінностей: а) особою (особами), що має вільний доступ до комп'ютерної техніки; б) особою (особами), що не мають вільного доступу до комп'ютерної техніки; 4) злочин вчинено з метою порушення авторських прав: а) особою (-ами), що має вільний доступ до комп'ютерної техніки; б) особою (-ами), що не має

вільного доступу до комп'ютерної техніки; 5) злочин вчинено з метою порушення алгоритму обробки інформації, знищення або пошкодження комп'ютерних програм і баз даних, а так само їх носіїв: а) особою, що має доступ до комп'ютерної техніки; б) особою, що не має доступу до комп'ютерної техніки; в) знищення, пошкодження або порушення алгоритму обробки інформації сталося внаслідок збою або несправності в автоматизованій системі і не є комп'ютерним злочином» [85, с. 473].

А вже А. І. Кунтій виокремлює такі типові слідчі версії, що висуваються на початковому етапі розслідування кримінальних правопорушень у сфері використання ЕОМ: «…1) був факт неправомірного доступу до комп'ютерної інформації; 2) є факт інсценування злочину з метою приховання іншого злочину; 3) злочин учинено особою, яка має відношення та вільний доступ у приміщення фірми чи особи, стосовно яких учинено злочин; 4) злочин учинено сторонньою особою, яка має на- вики роботи з ЕОМ та їх системами; 5) злочин учинено групою осіб; 6) злочин учинено на замовлення конкурентів по бізнесу (фізичних чи юридичних осіб)» [71, с. 877-878]. Підтримуючи вищевказані позиції, на основі проаналізованих кримінальних проваджень спробуємо визначити криміналістичні версії, які можна висувати на початковому етапі розслідування кримінальних правопорушень, пов'язаних з використанням Інтернет-банкінгу:

– кримінальне правопорушення, пов'язане з використанням Інтернет-банкінгу, вчинене з метою отримання матеріальної вигоди «хакером»;

– кримінальне правопорушення, пов'язане з використанням Інтернет-банкінгу, вчинене з метою отримання матеріальної вигоди співробітником певної установи, яка володіє навичками роботи з комп'ютерною технікою;

– кримінальне правопорушення, пов'язане з використанням Інтернет-банкінгу, вчинено з метою заволодіння інформацією з обмеженим

доступом особою (особами), що має вільний доступ до визначеної комп'ютерної техніки;

– кримінальне правопорушення, пов'язане з використанням Інтернет-банкінгу, вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що не має вільного доступу до визначеної комп'ютерної техніки;

– кримінальне правопорушення, пов'язане з використанням Інтернет-банкінгу, вчинено з метою порушення алгоритму обробки даних, знищення або пошкодження комп'ютерних програм і баз даних, а так само їх носіїв.

На основі вивчення матеріалів кримінальних проваджень [Додаток А] виокремлено найбільш поширені процесуальні дії початкового етапу розслідування досліджуваної категорії протиправних діянь, а саме:

– огляд місця події (98 %), огляд електронної інформації (94 %);

– обшук (91 %);

– призначення та проведення експертиз (100 %);

– тимчасовий доступ до речей і документів (79 %);

– огляд документів (53 %), допит потерпілих та свідків (100 %).

Зі свого боку, В. В. Корнієнко та В. І. Стреляний засвідчують те, що керівник слідчо-оперативної групи має заздалегідь підготуватися до проведення слідчих (розшукових) дій. Адже, на думку науковців, варто ретельно вивчити, до прикладу, територіальне розташування банку, визначити в якому приміщенні банк знаходиться: у вбудованому, прибудованому, окремо розташованій будівлі, вивчити входи-виходи (основні й запасні), кількість місцезнаходження пунктів обміну валют. Крім того, автори вказують, що потрібно чітко з'ясувати «…розташування внутрішніх приміщень банку: сховища; спеціальної каси; каси перерахунку; вечірньої каси; операційного залу; центру автоматизованої обробки інформації (комп'ютерного центру-серверу, архівування, модему «Банк-клієнт»); приміщень, де знаходяться індивідуальні сейфи для зберігання цінностей; кабінетів

керівництва банку, головного бухгалтера (знати в яких кабінетах працюють комп'ютери, які включено в мережу); підсобних приміщень, особливо приміщень перед сховищами (їх треба оглядати ретельно); складських приміщень» [62, с. 47-48].

В свою чергу, О. І. Мотлях відмічає, що «Початковий етап розслідування комп'ютерних злочинів вимагає належного відношення до підготовки та порушення кримінальних справ, пов'язаних з інформаційними технологіями. Особлива роль на цьому та інших етапах розслідування відводиться формуванню висококваліфікованої слідчої та оперативно-розшукової групи. Недоцільно, щоб спеціалістами у сфері високих технологій при процесуальних заходах були запрошені сторонні особи, оскільки вони не вболіватимуть за результативність справи. Осередком сформованої слідчо-оперативної групи та фахівців у зазначеній сфері мають бути особи з числа штатних працівників правоохоронних органів. Понятими ж слід запрошувати осіб, які б хоча мінімально володіють знаннями операційних комп'ютерних систем» [93, с. 16].

А вже О. В. Курман вказує на те, що незаконне втручання в роботу електронно-обчислювальної техніки та комп'ютерних мереж можливо за наявності наступних умов: «…1) володільцем інформації повинні бути визначені умови та правила отримання і обробки інформації; 2) власник (розпорядник) електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи оператор (провайдер) мереж електрозв'язку повинні розробити заходи захисту інформації в системі; 3) власник (розпорядник) комп'ютерів, систем та оператор (провайдер) мереж повинні розробити правила роботи системи; 4) між власником (оператором, провайдером) системи та володільцем інформації повинен бути укладений договір щодо захисту інформації в системі; 5) злочинець виконав хоча б одну із операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації» [79, с. 247].

Доречною в розрізі нашого дослідження вважаємо позицію Д. В. Пашнєва та М. Г. Щербаковського, які визначають, що «після прибуття на місце слідчий повинен вжити таких попереджувальних заходів, які забезпечують цілісність і незмінність інформації на комп'ютерному носії: – захистити й узяти під охорону приміщення, в якому перебувають засоби комп'ютерної техніки; – віддалити людей від обладнання та джерел живлення; – виявити стан комп'ютерної техніки (вимкнена або увімкнена); – переконатися, що за жодних обставин вимкнений комп'ютер не буде ввімкнено. Під час проведення огляду (обшуку) спеціаліст безпосередньо надає допомогу слідчому: – у виявленні засобів комп'ютерної техніки, її окремих компонентів, документації та інших об'єктів, які можуть містити сліди неправомірних дій; – у коректному (з точки зору збереження слідів злочину) відключенні засобів комп'ютерної техніки від енергопостачання; – в описі засобів комп'ютерної техніки, її окремих компонентів і документації, що вилучаються, у протоколі та додатках до нього; – у вирішенні питання щодо складу комплекту комп'ютерної техніки або окремих її компонентів, які підлягають вилученню або ізолюванню від вільного доступу; – у підготовці засобів комп'ютерної техніки до транспортування (їх упаковуванні, опечатуванні)» [73, с. 264-265]. І дійсно, під час розслідування кримінальних правопорушень, пов'язаних з використанням Інтернет-банкінгу, потрібно максимально забезпечити збереження інформації, яка перебуває на флеш-накопичувачах, жорстких дисках, кеш-пам'яті відповідного пристрою, в хмарних сховищах тощо.

З огляду на зазначене, вбачаємо вірною думку В. В. Корнієнка та В. І. Стреляного, які визначили наступний порядок роботи слідчої-оперативної групи: «1) ретельно вивчити план приміщення банку з розташуванням всіх внутрішніх кабінетів (безпосередньо на місці); 2) за необхідності забезпечити охорону основних і запасних входів та виходів; 3) ознайомитися з документами, що визначають організаційну структуру банку, положенням про управління (відділи), наказом про розподіл обов'язків

між керівництвом, ліцензією на здійснення операцій видану НБУ; 4) забезпечити присутність посадових осіб банку, а в окремих випадках – присутність представників НБУ. Під час проведення слідчих дій необхідно: 1) забезпечити присутність працівників на своїх робочих місцях (не допускати відходу з робочого місця жодного з працівників); 2) здійснювати ретельний контроль за касирами (буквально, за рухами рук, місцем знаходження їх особистих речей (сумок)); 3) контролювати дії працівників центру автоматизованої обробки інформації, не допускаючи здійснення операцій в момент проведення слідчих дій, а також усіх працівників, які працюють за комп'ютерами, що включені в мережу; 4) оглянути приміщення банку на предмет виявлення комп'ютерної техніки, яка може «нелегально» працювати від імені фіктивної фірми; 5) спостерігати за телефонним зв'язком, бо працівник банку може дати команду про списання коштів з будь-якого рахунку банківської установи чи підприємства; 6) забезпечити зовнішнє спостереження за банком (вікнами) і внутрішню охорону входу-виходу основного й запасного, забезпечуючи тільки вхід бажаючих до банку; 7) у ході огляду в приміщені операційного залу швидко виявити за роздруківкою фіктивні фірми за такими ознаками: фірми з великими оборотами, що почали працювати протягом останнього часу (від 1-3 днів до 2-3 місяців). Після встановлення осіб директора та головного бухгалтера цих фірм визначити відповідність даних, що знаходяться в банку за даними адресного бюро (чи не були раніше загублені чи викрадені документи, що пред'явлені при відкритті рахунку). Перевірити, чи знаходиться фірма за юридичною адресою відповідно до банківських документів. 8) у разі виникнення підозри необхідно відразу припинити рух безготівкових коштів в частині проведення витратних операцій на рахунках банку (поточних, розрахункових, депозитних; у національній валюті, іноземній валюті) одночасно по всім підрозділам» [62, с. 49].

Зі свого боку, К. Д. Заяць зазначає, що напрями розслідування слід визначати відносно джерел доказів про шахрайства. Серед них автор

виокремлює наступні: «…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 [45, с. 89].

В свою чергу, А. І. Кунтій вказував, що «…організація та технологія проведення огляду в справах про «комп'ютерні» злочини відрізняються від аналогічної слідчої (розшукової) дії під час розслідування традиційних злочинів. Це обумовлено не тільки небезпекою навмисного знищення інформації, яка має доказове значення, з боку ще не виявлених учасників злочину, інших зацікавлених осіб, але і необережним поводженням слідчого й інших членів слідчо-оперативної групи, які можуть зашкодити інформації, знищити сліди внаслідок неправильного, некваліфікованого поводження з програмно-апаратними засобами. Однією з найважливіших умов проведення огляду є суворе дотримання встановлених правил поводження з комп'ютерною технікою та носіями інформації, технічно грамотне проведення пошуку доказів, потрібної інформації. Також рекомендується

обов’язково залучати до огляду спеціаліста в галузі інформатики та обчислювальної техніки. Нагадаємо, що лише огляд місця події у виняткових випадках, може бути проведений до внесення відомостей про кримінальне правопорушення до ЄРДР і після завершення такого огляду, слідчий, прокурор зобов’язаний негайно внести такі відомості до ЄРДР. Саме ця слідча (розшукова) дія сприяє вирішенню низки важливих питань, а саме: – на якому об’єкті (на якому конкретно комп’ютері, в якому структурному підрозділі установи) сталася подія; – до якого виду можна віднести комп’ютерний злочин, що відбувся; – яким способом учинено злочин; – які сліди, чи інші речові докази вказують на причетність до злочину певної особи; – яким є під час огляду стан засобів захисту інформації, охорони приміщень, обладнання та низка інших питань» [71, с. 879-880].

Досить вірним вважаємо твердження А. В. Реуцького, який виокремив наступні об’єкти огляду місця події, а саме: «…приміщення: (а) де обслуговуються розрахунки платіжними картками; (б) де знаходиться банкомат; (в) банківських установ або процесингових центрів; (г) де виготовлялися підроблені платіжні картки; (д) де встановлена комп’ютерна техніка, за допомогою якої вчинено злочин, або де знаходиться провайдер, що надає послуги доступу в мережу Інтернет; а також (е) ділянки території, по яких проходять кабелі зв’язку між учасниками системи, які обслуговують обіг платіжних карток, та ін.» [120, с. 126].

На основі дослідження матеріалів кримінальних проваджень [Додаток А] нами було встановлено місця, які найчастіше підлягають огляду на початковому етапі розслідування, зокрема: робоче місце потерпілого, робоче місце підозрюваного, банкомати, місця доступу до загальної мережі Wi-Fi та ін.

Стосовно проведення обшуку в досліджуваній категорії кримінальних проваджень, то ми поділяємо позицію І. О. Коваленка, який виділяє ряд особливостей під час нього. Автор зазначає, що в першу чергу потрібно звернути на комп’ютерну техніку, що знаходиться в приміщенні, а також на

стан інтернет-мережі, при огляді приміщення слід провести пошук портативних USB флеш-накопичувачів, в тому числі замаскованих. Дослідник наголошує, що не аби яке значення має виявлення мобільного телефону, планшету на місці проведення обшуку, адже, як правило, на них може знаходитись дуже важлива інформація, яка слугуватиме швидкому розслідуванню протиправного діяння. Крім того, науковець акцентує увагу, що вказана техніка перед вилученням повинна бути правильно упакована та опечатана і також важливо до потрапляння в приміщення відключити його від електромережі, що унеможливить швидке знищення інформації, яка знаходиться на електронних носіях. Як приклад, І. О. Коваленко зауважує, що зловмисники за допомогою мікрохвильової печі можуть знищити будь-який електронний носій за лічені секунди. Автор робить слушний висновок, що досліджуваний вид протиправного діяння суттєво відрізняється від інших тим, що головною його ознакою є використання всесвітньої мережі Інтернет з залученням ЕОТ [56, с. 117].

Серед особливостей проведення обшуку, пов’язаного з комп’ютерною технікою, А. І. Кунтій виокремлює наступні: «…1) використання принципу раптовості під час прибуття та входження до приміщення, в якому буде проводитись обшук, або в якому знаходиться комп’ютерна техніка, що підлягає обшукові; 2) об’єктом пошуку є не тільки технічний пристрій чи матеріальний носій комп’ютерної інформації, якими можуть бути жорсткий диск комп’ютера, дискета, оптичний диск, флеш-карта тощо, а й інформація, яка зберігається на них і яка, власне, й є основним об’єктом пошуку та вилучення з метою встановлення обставин учинення комп’ютерного злочину; 3) місцем проведення слідчої дії в такому разі буде не просто приміщення, в якому є носій комп’ютерної інформації, а приміщення, технічний засіб та інформаційний масив конкретного комп’ютерного об’єкта; 4) вилучення комп’ютерних об’єктів, що містять інформаційні дані, може здійснюватися по-різному. Можуть бути вилучені носії інформації або навіть комп’ютерна система загалом чи окремі її частини, якщо дані не можуть бути доступі для

їх копіювання або вивчення на іншому обладнанні. Для відновлення таких даних потрібні спеціальні програми, інколи – додаткове обладнання, а сам процес відновлення може займати чимало часу. В цих випадках провадити фактично дії з дослідження програмного продукту під час проведення обшуку або виїмки не доцільно. За певних обставин можна визнати припустимим вилучення даних шляхом їх копіювання на окремі носії інформації. В таких випадках необхідно вжити спеціальних заходів, що забезпечують цілісність і збереження вилучених даних, а використані для копіювання носії не повинні містити жодної інформації. Не доцільно копіювати вилучену інформацію на носії, що містять інформацію, яка стосується цієї справи і навіть, якщо ця інформація ідентична або містить фрагменти тієї, котра підлягає вилученню. Повинні бути створені умови та гарантії ідентичності копії оригіналу на момент провадження обшуку або виїмки та надійності її зберігання протягом усього розслідування; 5) неможливість використання у процесі пошуку тайників із магнітними носіями металошукачів або рентгенівської установки, оскільки їх застосування може призвести до знищення інформації на цих носіях; 6) необхідність швидко проаналізувати великий обсяг інформації, яку було виявлено під час проведення обшуку з метою встановлення її цінності для досудового слідства; 7) проведення обшуку лише на одному або декількох комп’ютерах, які входять до локальної комп’ютерної мережі» [71, с. 882-883].

Після потрапляння до місця проведення обшуку, як зазначають окремі науковці, уповноважена особа повинна запропонувати особі видати речі, які передбачені ухвалою слідчого судді, а також інші речі, які вилучені з цивільного обігу чи незаконно отримані. На початковому етапі обшуку важливого значення набуває встановлення психологічного контакту, що досягається через взаємне сприймання сторін та обмін як вербальною, так і невербальною (міміка, жести) інформацією. Такий контакт може бути започатковано, наприклад, коли слідчий перед обшуком пропонує віддати розшукувані об’єкти, мотивуючи це тим, що небажано, щоб діти,

повернувшись зі школи, спостерігали картину обшуку. Навіть за умови негативної відповіді такий крок може стати підґрунтям до встановлення подальшого контакту. Якщо обшукуваний тримається скуто, самовпевнено чи агресивно, такий стан можна спробувати зняти бесідою про родинні стосунки, роботу, стан здоров'я тощо [180, с. 148].

Ефективність обшуку зростає, як відмічає О. Л. Мусієнко у випадках, коли факт здійснення кримінального провадження невідомий правопорушникам. У цьому випадку провадження обшуків є для них раптовим. Одним із завдань обшуку є відшукання й вилучення викраденого майна: товарів, отриманих у магазинах, торговельних підприємствах злочинним шляхом за договором купівлі-продажу; продуктів сільськогосподарського виробництва, грошових коштів тощо. Вивчення слідчої практики показує, що своєчасне проведення обшуків з метою виявлення вилученого майна дало можливість не лише відшкодувати матеріальний збиток, але й одержати нові докази. Крім перерахованих об'єктів, відшукуванню підлягають, також документи й предмети (наприклад «ляльки», гральні пристрої та ін.), за допомогою яких підготовлявся й вчинявся злочин. Такими об'єктами можуть бути: документи, за допомогою яких відбувалися шахрайські дії по одержанню грошових коштів, предмети, за допомогою яких підроблялися документи, підроблені, а також викрадені печатки й штампи; всі інші предмети й документи, які можуть слугувати засобами для встановлення істини в справі (листи, фотознімки, приватні записи, чернетки, розписки тощо) [97, с. 129].

А вже О. І. Мотлях відмічає, що «…пошук предметів протиправної діяльності та осіб, причетних до вчинення злочинів – це досить трудомісткий процес, що вимагає спеціальних пізнань, значної кількості часу, фахової підготовленості, вміння на практиці застосовувати складні програмні апаратно-технічні засоби та ін. Побутує серед дослідників думка про знеструмлення приміщення перед початком обшуку чи виїмки як ефективний тактичний прийом слідчого, дисертантом така позиція авторів повністю

відкидається, оскільки це може призвести до не передбачуваних наслідків, у тому числі знищення інформації. Обґрунтовано, що при проведенні цих процесуальних заходів слід уникнути обшуку приміщення на предмет схованок за допомогою приладів, які містять у собі магнітні носії – це також призведе до руйнування електронної інформації» [95, с. 61].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] окреслено перелік об'єктів, які необхідно вилучати під час обшуку:

1) електронно-обчислювальна техніка, за допомогою якої здійснювалось втручання в роботу інтернет-мереж для їх дестабілізації або отримання відомостей, необхідних для реалізації операцій в інтернет-банкінгу (комп'ютери, планшети, ноутбуки, смартфони);

2) реквізити карток, що викрадені з серверів магазинів електронної торгівлі, платіжних і розрахункових систем, з персональних ґаджетів користувачів;

3) фотографії, відеозаписи, на яких наявні дані, що мають значення для кримінального провадження;

4) квитанції про здійснення банківських операцій;

5) смартфони або інші ґаджети, в яких наявна адресна книга (ПІБ й адреси клієнтів фінансових установ, підприємств та організацій різних форм власності);

6) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб та ін.

Відносно тактичних прийомів обшуку, ми підтримуємо позицію С. В. Чучка, який серед них виділив найбільш ефективні, як-от: «видалення підозрюваного з місця проведення обшуку; залучення підозрюваного до участі в процесуальній дії; зіставлення інформації, яка міститься у відповідях обшукуваного; застосування технічних засобів. До тактичних прийомів відноситься і спосіб обміну інформацією між тими, хто проводить обшук, і манера їхнього поводження… Оскільки обшукуваний, члени його сім'ї виявляються психологічно неготовими до протидії розслідуванню, їм важче

приховати хвилювання. Часто в цих осіб немає достатньо часу для вжиття тих чи інших засобів маскування чи знищення предметів пошуку» [172, с. 124-125].

Також з'ясовано, що на початковому етапі розслідування необхідно максимально забезпечити збереження інформації, яка перебуває на флеш-накопичувачах, жорстких дисках (носіях), кеш-пам'яті відповідного пристрою, в хмарних сховищах та ін. Для цього обов'язково потрібно застосовувати проведення одночасних обшуків за різними адресами ймовірного знаходження правопорушників.

Наостанок зазначимо, що під час проведення обшуку виникає необхідність вилучати як заблоковані, так і розблоковані переносні ґаджети (смартфони, smart-годинники, портативні відео-реєстратори, GPS-навігатори). Звісно, специфіка їх вилучення відрізняється, адже з розблокованих пристроїв в принципі достатньо дістати, якщо вони є, SIM-карту та карту пам'яті, тоді як заблоковані потрібно ще розблокувати перед вилученням відповідних слотів. А для цього варто залучити для обшуку спеціаліста в галузі комп'ютерних технологій.

Відносно проведення НСРД для початку звернемось до дисертації І. О. Коваленка. На основі вивчення матеріалів кримінальних проваджень, дослідник визначив, що «…специфічною ознакою шахрайства в сфері використання банківських електронних платежів є потреба проведення цілого ряду НСРД та оперативно-технічних заходів, пов'язаних із встановленням шахрая та його зв'язків. Зокрема, серед них необхідно виокремити такі як спостереження за об'єктом або особою; огляд кореспонденції; прослуховування телефонних переговорів; зняття інформації з транспортних та електронних систем. На основі аналізу матеріалів кримінальних проваджень, нами було виявлено наступні труднощі, що виходять з реалізації відомостей НСРД при розслідуванні шахрайства в сфері банківських електронних платежів, наприклад: незлагоджена взаємодія підрозділів правоохоронних органів та працівників установ зв'язку (69 %);

проблематичність одержання ухвали слідчого судді апеляційного суду стосовно проведення певної НСРД (61 %); відсутність бажання окремих уповноважених осіб покращувати процес кримінального провадження, а також потяг до пошуку більш легких шляхів для отримання доказової інформації (32 %); брак потреби в огляді та вилученні документів (48 %)» [157, с. 157-158]. Ми також підтримуємо вказану позицію та вважаємо, що для визначення місць перебування вказаних осіб необхідно організувати та провести низку НСРД, серед яких виділено спостереження за об'єктом та прослуховування телефонних переговорів.

Ми поділяємо твердження окремої групи науковців, які зазначають наступне: «Аудіоконтроль особи полягає у прослуховуванні та фіксації розмов, що відбуваються на відповідних об'єктах. Аудіоконтроль особи проводиться за допомогою спеціальних технічних засобів фіксації інформації. Безпосередній порядок проведення такої НСРД визначається відповідними відомчими нормативно-правовими актами. Аудіоконтроль особи може здійснюватися епізодично (наприклад, на певний проміжок часу проведення зустрічі) та неперервно (на весь проміжок часу проведення цієї дії, визначений в ухвалі слідчого судді). Відеоконтроль особи здійснюється технічними засобами, що забезпечують негласне візуальне спостереження за діями, розмовами, поведінкою підозрюваного, обвинуваченого та осіб, що контактують з ними у зв'язку з їх протиправною діяльністю. Відеоконтроль обстановки та дії осіб, їх фіксація може відбуватися в житлі або іншому володінні особи, а також у приміщеннях, транспортних засобах та інших місцях, які не належать до житла та не є іншим володінням особи. Відеоконтроль особи, як правило, здійснюється спеціальними підрозділами, що забезпечують впровадження та експлуатацію СТЗ. Посадова особа уповноваженого оперативного підрозділу правоохоронного органу, якій було доручено аудіо-, відеоконтроль особи, негайно після завершення цієї НСРД повідомляє про це слідчого та надає йому для дослідження інформацію, отриману при застосуванні технічних засобів. Слідчий, а в разі необхідності

спеціаліст відповідно до вимог ст. 266 КПК вивчає зміст отриманої інформації, про що складає протокол» [50, с. 161-162]. Як вже було зазначено, вказані НСРД дійсно мають важливе значення для кримінальних проваджень досліджуваної категорії.

«З огляду на це, на нашу думку, в кожному конкретному випадку під час оцінки допустимості доказів (якщо злочин було перекваліфіковано на менш тяжкий) суду необхідно детально вивчати всі матеріали кримінального провадження на предмет того, чи була об'єктивна можливість визначення правильної кваліфікації кримінального правопорушення перед початком проведення НС(Р)Д. Або також можливий випадок, коли в ході проведення НС(Р)Д отримано нові докази, які вказують на інший склад кримінального правопорушення. Тому не можна однозначно визнавати докази, отримані в результаті НС(Р)Д, недопустимими на підставі зміни кваліфікації злочину на менш тяжкий. Таким чином, усі визначені питання є дискусійними та потребують подальших наукових досліджень. Вважаємо, що їх врахування під час оцінки доказів у кримінальному провадженні на предмет допустимості сприятиме додержанню прав його учасників, підвищенню якості роботи правоохоронних органів та додержанню законності під час прийняття судових рішень з огляду на преюдиціальне значення рішень інших судів у питаннях допустимості доказів» [30, с. 189].

Підводячи підсумок відносно особливостей проведення НСРД, підкреслимо важливість детального огляду вилучених за результатами їх проведення смартфонів, сітьового та серверного обладнання, комп'ютерної техніки, а також її комплектуючих (процесорів, модулів пам'яті, жорстких дисків).

Стосовно специфіки підготовчого етапу до допиту у справах щодо шахрайства, цікавою є думка Н. В. Павлової, яка зазначає, що у слідчого виникає необхідність ознайомлення з низкою документів, використаних під час вчинення злочину даної категорії, та відбору серед них тих, що можуть застосовуватися під час провадження допиту. Авторка наголошує, що з метою

з’ясування картини злочину в цілому слідчий повинен вивчити матеріали кримінального провадження та уважно проаналізувати зміст документів, які відображають факт укладення угоди щодо відчуження житла. У зв’язку з цим слідчому необхідно звернутися до процедури укладення угоди щодо відчуження житла та її правової регламентації. На підставі вивчення матеріалів кримінального провадження та документів, що містяться в ньому, слідчий повинен встановити: які дії, що вчинювалися під час укладення угоди, є незаконними, в чому вони полягають; які особи їх вчинили, коли і в якому місці; які нормативні акти, що регулюють порядок здійснення правочинів щодо житла, порушувалися тощо. Для вирішення вказаних питань вже на стадії підготовки до допиту щодо злочинів вказаної категорії необхідно залучити спеціалістів у сфері обігу житла. Вони можуть допомогти правильно оцінити докази, роз’яснити факти, що мають значення для справи, скласти приблизний перелік питань, які необхідно з’ясувати у ході допиту [101, с. 122].

На основі узагальнення матеріалів кримінальних проваджень [Додаток Б] було з’ясовано, що допит потерпілих та свідків проводився у 100 % випадків.

Встановлено, що до проведення допиту потерпілих необхідно оглянути наявну в них електронно-обчислювальну техніку (смартфони, ноутбуки, планшети), за допомогою якої відбувалася переписка чи розмова з правопорушником.

У свою чергу, окрема група науковців (М. М. Єфімов, Н. В. Павлова, С. В. Чучко) вірно зазначила, що «…у потерпілого від шахрайства при купівлі-продажу товарів через мережу Інтернет обов’язково необхідно досліджувати питання стосовно наступних обставин: відповідний процес знаходження Інтернет ресурсу шахрая (рекомендація знайомих; спам-розсилка); спосіб спілкування з шахраєм (лише на сайті; на сайті і телефоном; через певні соціальні мережі); речі, які потерпілий бажав придбати; спосіб оплати» [34, с. 147].

З огляду на зазначене, було зосереджено увагу на допиті потерпілого та окреслено основні його завдання:

– з'ясувати обставини вчинення протиправного діяння (час, місце, зокрема, з доступом до загальної мережі Wi-Fi, наявність поблизу сторонніх осіб – можливість віддаленого підключення з іншого ґаджету);

– проаналізувати його передумови (чи були надіслані на номер потерпілого та прийняті повідомлення – в якому месенджері та якого змісту, чи були наявні дзвінки – в якому месенджері та якого змісту);

– встановити послідовність дій потерпілого після вчинення кримінального правопорушення (одразу повідомив в правоохоронні органи чи своїм знайомим, родичам, що зробив з ґаджетом – вимкнув, перезавантажив, продовжив користуватися).

З приводу допитів в якості свідків окремих категорій осіб звернемось до позиції А. І. Кунтія. Адже автор досить точно виокремив декілька специфічних груп свідків та обставини, які потрібно у них з'ясовувати. Зокрема, дослідник сформулював наступні рекомендації: «Під час допитів операторів ЕОМ варто з'ясувати: правила ведення журналів операторів, порядок прийому-здачі змін, режим роботи операторів; порядок ідентифікації операторів; правила експлуатації, збереження, знищення комп'ютерних роздруківок, категорію осіб, що мають до них доступ; порядок доступу в приміщення, де знаходиться комп'ютерна техніка... У процесі допитів програмістів з'ясовується: перелік використовуваного програмного забезпечення в установі, щодо якої було вчинено злочин, його класифікація (ліцензійне чи власного виробництва); паролі захисту програм, окремих пристроїв комп'ютера, частота їхніх змін; технічні характеристики комп'ютерної мережі (у разі її наявності), хто є адміністратором мережі… У співробітника, що відповідає за інформаційну безпеку, чи адміністратора комп'ютерної мережі (за їх наявності) з'ясовують: наявність спеціальних технічних засобів захисту інформації; порядок доступу користувачів у комп'ютерну мережу; порядок ідентифікації користувачів комп'ютерів... У

співробітників, що займаються технічним обслуговуванням обчислювальної техніки, з'ясовують: перелік і технічні характеристики засобів комп'ютерної техніки, встановлених в організації, а також перелік захисних технічних засобів; періодичність технічного обслуговування, проведення профілактичних і ремонтних робіт; відомості про випадки виходу, що відбулися за останній час, апаратури з ладу; випадки незаконного підключення до телефонних ліній зв'язку, установка якого-небудь додаткового електроустаткування» [71, с. 888-889].

Як підсумок, було визначено, що під час допиту потерпілого або свідка доцільно демонструвати певні об'єкти:

а) скріншоти повідомлень переписки зі злочинцем;

б) зображення (скріншот) документу, який підтверджує зняття коштів з рахунку потерпілого;

в) виписку з банківського рахунку потерпілого;

г) у випадках розмови зі злочинцем в телефонному режимі чи в режимі відео-конференції з'ясувати у потерпілого чи зробив він її запис – якщо так, то долучити до кримінального провадження для подальшого використання під час проведення пред'явлення для впізнання.

Констатуючи вищенаведене, зазначимо, що початковий етап акумулює процесуальні дії, необхідні для максимального збору доказової інформації на початку кримінального провадження. Визначено криміналістичні версії, які висуваються на початковому етапі розслідування кримінальних правопорушень. Встановлено, що під час розслідування досліджуваної категорії протиправних діянь проводяться різноманітні процесуальні дії, серед яких найбільш важливими, на нашу думку, є такі як огляд місця події та ЕОТ, обшук, НСРД, допит потерпілих та свідків.

3.2. Подальший етап розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу

Подальший етап розслідування починається, як вважає більшість вчених-криміналістів, з моменту пред’явлення підозри. Ми підтримуємо цю позицію, тому відповідно всі слідчі (розшукові) дії, негласні слідчі (розшукові) дії та інші процесуальні дії, а також розшукові заходи при розслідуванні кримінальних правопорушень, пов’язаних із 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 [188, с. 89].

Стосовно визначення початку подальшого етапу розслідування то, наприклад, О. М. Дуфенюк доречно вказує, що він розпочинається тоді, коди проведено комплекс першочергових і невідкладних слідчих (розшукових) дій після внесення відомостей до ЄРДР та початку досудового розслідування. Автор наголошує, що залежно від того, які результати під час проведення невідкладних слідчих (розшукових) дій отримано, можна вирізнити два напрями розслідування. Відносно першого напряму, коли протиправне діяння розкрито та встановлено особу правопорушника, науковець вказує, що він охоплює ухвалення процесуального рішення – повідомлення про підозру в порядку, передбаченому ст. 278 КПК України, активізацію зусиль над закріпленням доказів винуватості особи; встановлення обставин події кримінального правопорушення, зокрема тих, які пом’якшують чи обтяжують відповідальність; застосування заходів забезпечення кримінального провадження, зокрема обрання запобіжних заходів; проведення негласних слідчих (розшукових) дій. З приводу другого напряму, (у випадках, коли кримінальне правопорушення не розкрито) дослідник зауважує, що він

характеризується активізацією зусиль над пошуком криміналістично значущої інформації про подію та його учасників, збиранням, дослідженням уже виявлених доказів, перевіркою висунутих версій тощо. Як висновок, О. М. Дуфенюк говорить про те, що у такому разі типовим є проведення повторних та додаткових слідчих (розшукових) дій, надання доручень оперативним підрозділам, скерування запитів до підприємств, установ та організацій тощо, проведення негласних слідчих (розшукових) дій тощо [71, с. 512].

Зі свого боку, О. І. Мотлях вказує, що «…подальший етап розслідування комп'ютерних злочинів, як і іншої категорії злочинів, залежить від змісту отриманих даних на початковому етапі розгляду справи. Виходячи з змісту слідчих ситуацій, що склалися, автор робить висновок про наявність попереднього зговору, кількісний склад учасників злочину, їх ієрархічну будову та розподіл ролей між суб'єктами вчиненої протиправної дії. На цьому етапі слідчому доведеться працювати з іншими суб'єктами, що не фігурували у справі, яка розслідується. Насамперед – це нові свідки, потерпілі, підозрювані, обвинувачені тощо. З'являться у справі й інші речові докази, які підсилять доказове значення окремих обставин злочину. Якісного змісту набудуть подальша організація планування розслідування справи, висунення та відпрацювання криміналістичних версій, проведення окремих слідчих дій та ін.» [93, с. 13].

В свою чергу, А. Ф. Волобуєв відносно подальшого етапу розслідування висловив наступні твердження. Зокрема, автор зазначив, що вказаний етап починається з моменту повідомлення особі про підозру у вчиненні протиправного діяння. А серед головних завдань цього етапу розслідування науковець виокремив наступні: «…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)».

Крім того, дослідник вказував на те, що у кожній окремій методиці розслідування на цьому етапі розглядаються типові слідчі ситуації та комплекси слідчо-розшукових дій, що їм відповідають. А типові слідчі ситуації, на думку А Ф. Волобуєва, визначаються позицією, яку займає особа, якій було повідомлено про підозру у вчиненні кримінального правопорушення [73, с. 13].

З приводу досліджуваної категорії кримінальних проваджень, найбільш точно сформулювали необхідні процесуальні дії подальшого етапу розслідування Д. В. Пашнєв та М. Г. Щербаковський. Автори надали наступний перелік: «…обшуки з метою вилучення засобів комп'ютерної техніки, за допомогою яких був здійснений злочин (у разі опосередкованого мережевого доступу злочинця до комп'ютера), а також носіїв комп'ютерної інформації, здобутої унаслідок злочину: паперові роздруківки, вінчестери системних блоків, компакт-диски, флеш-пам'ять тощо; – призначення комп'ютерно-технічної експертизи після виявлення перерахованих об'єктів та їх огляду; – важливим засобом перевірки й підтвердження свідчень підозрюваного є проведення з його участю слідчого експерименту; цілями якого є підтвердження наявності в особи професійних навичок роботи з комп'ютерними засобами, програмування та вміння здійснити несанкціонований доступ, перевірки можливості здійснити несанкціонований доступ у певний спосіб або за допомогою певних засобів; слідчий експеримент на певному місці проводиться для підтвердження перебування особи у визначеному місці, пов'язаному з підготовкою і скоєнням злочину або приховуванням його слідів; – допити свідків, зокрема вказаних підозрюваним для перевірки його показань» [73, с. 264-265].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] було з'ясовано, що на подальшому етапі розслідування переважно проводяться такі СРД:

– допит підозрюваних (100 %);

– одночасний допит раніше допитаних осіб (82 %);

– призначення та проведення експертиз (100 %);

– пред’явлення для впізнання за голосом (3 %) та в натурі (1 %).

Розглянемо почергово кожну з них. Для початку розглянемо пред’явлення для впізнання як ймовірну СРД, яка проводиться в обмеженій категорії проваджень. Відповідно до ч. 1 ст. 228 КПК України «…перед тим, як пред’явити особу для впізнання, слідчий, прокурор попередньо з’ясовує, чи може особа, яка впізнає, впізнати цю особу, опитує її про зовнішній вигляд і прикмети цієї особи, а також про обставини, за яких вона бачила цю особу, про що складає протокол. Якщо особа заявляє, що вона не може назвати прикмети, за якими впізнає особу, проте може впізнати її за сукупністю ознак, у протоколі зазначається, за сукупністю яких саме ознак вона може впізнати особу. Забороняється попередньо показувати особі, яка впізнає, особу, яка повинна бути пред’явлена для впізнання, та надавати інші відомості про прикмети цієї особи» [75].

В свою чергу, окрема група вчених-криміналістів надали наступне визначення поняття пред’явлення для впізнання, а саме, що «…це слідча дія, що полягає у пред’явленні особі об’єктів, які вона спостерігала раніше, у зв’язку з подією злочину з метою встановлення їхньої тотожності чи групової належності. Загальними підставами для пред’явлення для впізнання є: заява особи під час допиту про те, що вона може впізнати об’єкт, який спостерігала раніше, і добре пам’ятає його ознаки та відмінності; під час допиту особа називає лише загальні риси об’єкта, не може точно описати його відмінності, але висловлює впевненість, що зможе його впізнати, коли побачить» [68, с. 183].

Як й усі СРД пред’явлення для нараховує три етапи: підготовка до його проведення; робочий етап (безпосереднє проведення впізнання); заключний етап (фіксація результатів СРД). З приводу підготовчого етапу, то ми підтримуємо перелік заходів, наведений К. О. Чаплинським, як-от: попередній допит особи, яка впізнає; визначення місця, часу та способу проведення впізнання; створення оптимальних умов для проведення

визначеної СРД; підбір статистів і понятих; визначення способу фіксації ходу та результатів впізнання (відеозйомка чи фотографування); підготовка потрібних техніко-криміналістичних засобів; забезпечення охорони правопорушників, які знаходяться під вартою; інструктаж усіх учасників досліджуваної СРД [161, с. 34].

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).

Під час допиту підозрюваного, як точно відмічає А. І. Кунтій, варто встановити наступні обставини: «…1) де і ким він працює; 2) до якої комп'ютерної інформації має доступ, які операції з інформацією він має право поводити; 3) який його рівень підготовки як програміста, досвід роботи зі створення програм, які мови програмування він знає; 4) які ідентифікаційні коди та паролі закріплені за ним; 5) до яких видів програмного забезпечення він має доступ; 6) які операції він виконував у досліджуваний час; 7) з якого джерела або від кого він дізнався про інформацію, що зберігається на комп'ютері; 8) від кого була отримана інформація про засоби захисту комп'ютерної інформації, які способи для їх подолання; 9) як вчинявся неправомірний доступ, які засоби для цього застосовувалися; 10) кому була передана (або планувалося передати) отриману інформацію, з якою метою; 11) яку мали мету під час учинення злочину, яка матеріальна вигода за це була отримана; 12) як знищувалися сліди неправомірного доступу до комп'ютера; 13) як часто вчинявся неправомірний доступ до комп'ютерної інформації; 14) хто сприяв підозрюваному у вчиненні злочину й як» [71, с. 884-885].

З'ясовано, що під час допиту підозрюваних необхідно встановлювати наступні факти:

– електронно-обчислювальна техніка, яка була застосована для

вчинення протиправних діянь;

– програмне забезпечення, яке використовувалось для вчинення кримінального правопорушення (програми віддаленого доступу, «трояни», «боти»);

– логіни та паролі акаунтів, які використовувались для спілкування з потерпілими; реквізити банківських карт та рахунків, на які переказувались кошти.

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було з'ясовано, що під час проведення допиту підозрюваного можуть виникнути як безконфліктні (19 %), так і конфліктні ситуації (81 %). Відповідно до проведеного анкетування респондентів [Додаток Б] нами було встановлено наступні ситуації:

– підозрюваний за власним бажанням викладає правдиві відомості про обставини вчинення кримінального правопорушення, конфліктна ситуація відсутня (19 %);

– підозрюваний повідомляє інформацію про обставини протиправного, однак не висвітлює її у повному обсязі (26 %). Це відбувається через страх помсти зі сторони співучасників (45 %), через залежність від його організатора (21 %), заінтересованістю в результатах провадження (34 %);

– підозрюваний не бажає давати повні та щирі показання – факт конфліктної ситуації (29 %);

– підозрюваний цілком відмовляється від комунікації з уповноваженою особою, відмовляється давати показання, а також брати участь у проведенні окремих СРД (21 %);

– підозрюваний не заперечує факт і зміст протиправного діяння, однак спростовує свою участь у його вчиненні (5 %).

Для вирішення конфліктних ситуацій необхідно застосовувати відповідні тактичні прийоми. З цього приводу ми підтримуємо групу науковців (М. М. Єфімова, Н. В. Павлову, С. В. Чучка), які зазначили, що вони обираються залежно від слідчої ситуації: уповноважена особа може

застосовувати і пред'явлення доказів, і оголошення показань інших осіб, і методи переконання, і постановку деталізуючих, нагадуючих, контрольних запитань та ін. Крім того, автори зауважили, що у випадках, коли підозрюваний дає правдиві показання, завдання слідчого полягає в уточненні цих відомостей, максимальній деталізації показань та ін. Якщо ж він дає неправдиві показання, дослідники наголошують на потребі вжити заходів для викриття неправди: «…роз'яснити положення кримінально-процесуального законодавства про обставини, що пом'якшують вину, деталізувати його показання, провести повторні допити з тих самих обставин, пред'явити письмові і речові докази: документи, складені ним, експертні висновки, акти документальних ревізій, показання свідків, інших осіб тощо» [34, с. 148].

Щодо особливостей роботи в банківських установах ми підтримуємо позицію В. В. Корнієнка та В. І. Стреляного стосовно того, що уповноважена особа повинна враховувати специфіку добровільної участі працівників банку у вчиненні економічних протиправних діянь, пов'язаних зі здійсненням банківських операцій. Автори акцентують увагу на тому, що у цьому випадку недоцільно залучати осіб, підозрюваних у причетності до кримінального правопорушення, до проведення слідчих (розшукових) дій до моменту, коли всі необхідні докази його вини не будуть зібрані та проаналізовані. Адже, як вірно відмітили науковці, найважливішу роль на даному етапі має допит особи в якості підозрюваного. На останок, В. В. Корнієнка та В. І. Стреляного зробили висновок, що при цьому необхідно забезпечити всебічну та ретельну підготовку до допиту, у ході якої зібрати повну інформацію про причетність працівника банку до вчинення кримінального правопорушення [62, с. 67].

А вже К. О. Чаплинський на основі дослідження опитування респондентів встановив, що до найбільш розповсюджених тактичних прийомів допиту підозрюваного, які використовуються у правоохоронній практиці, відносяться наступні: «…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%» [162, с. 164-165].

Здійснення аналізу опитування респондентів [Додаток Б] дало змогу зробити висновок, що при розслідуванні кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, вони вбачають потребу та можливість в застосовуванні таких тактичних прийомів:

– створення уявлення про інформованість уповноваженої особи – 89 %;

– швидкий темп допиту – 56 %;

– використання фактора раптовості – 57 %;

– створення напруги – 69 %;

– пред'явлення речових доказів – 33 %;

– застосування відеозапису – 45 %.

Найбільш ефективним серед них слід вказати пред'явлення речових доказів, серед яких можуть демонструватись наступні об'єкти:

– свідчення потерпілих;

– протоколи пред'явлення для впізнання з позитивним результатом (підозрюваного впізнано за голосом чи в натурі);

– флеш-накопичувачі та жорсткі диски з інформацією про банківські операції з грошовими коштами;

– скріншоти хмарних сховищ;

– скріншоти переписки з потерпілими.

Для прикладу, 25 грудня 2020 року гр. Д., перебуваючи у будинку №17, в селі Лохово, Мукачівського району, за місцем проживання гр. Л., діючи умисно, маючи злочинний умисел спрямований на заволодіння грошових

коштів, таємно, з корисливих спонукань, усвідомлюючи протиправний характер своїх дій та настання суспільно небезпечних наслідків та їх карність, дізнавшись реквізити банківської картки ПАТ КБ «Приватбанк», яка належить вищезазначеному потерпілому , та використовуючи його мобільний телефон, незаконно використав реквізити його картки для проходження «IVR»-опитування за допомогою мобільного зв`язку, шляхом звернення на номер «3700» та обрання відповідної послуги у голосовому меню, чим здійснив несанкціонований вхід в автоматизовану систему АТ КБ «Приватбанк», що призвело до витоку, інформації, яка в ній оброблюється. Крім цього, в період часу з 28 грудня 2020 року по 29 грудня 2020 року гр. Д., користуючись тим, що його дії непомічені сторонніми особами та достовірно знаючи де потерпілий зберігає свою банківську картку та лист із записаним паролем її авторизації взяв вказану банківську картку та мобільний телефон потерпілого. В подальшому правопорушник, користуючись мобільним телефоном потерпілого пройшовши «IVR»-опитування та в подальшому здійснив набір цифр на телефоні гр. Л. для підтвердження здійснення чотирнадцяти операцій переказу грошових коштів на загальну суму 4428 гривень [145]. На початку першого допиту підозрюваний повністю заперечував свою вину. В процесі пред’явлення доказів (скріншоти банківських операцій, показання потерпілого, де він знаходився в цей час тощо) гр. Д. змінив конфліктну ситуацію на безконфліктну – почав викладати правдиві відомості про обставини вчинення кримінального правопорушення.

На основі опрацювання матеріалів кримінальних проваджень нами було з’ясовано, що для усунення розбіжностей у показаннях потерпілих, свідків та підозрюваних у досліджуваній категорії кримінальних проваджень у 82 % випадках здійснювався одночасний допит двох або більше осіб.

Відносно визначеної процесуальної дії ми підтримуємо позицію групи дослідників (М. М. Єфімов, Н. В. Павлова, С. В. Чучко), які наголосили на доцільності її проведення у наступних випадках: «…1) якщо особа, яка надає правдиві показання, має вплив на іншу та здатна сприяти у ході одночасного

допиту зміні її позиції; 2) між особами, одна з яких надає правдиві показання, а інша добросовісно помиляється стосовно них в силу певних обставин; 3) між підозрюваним, який надає правдиві показання, та свідком, який, на думку уповноваженої особи, надає завідомо неправдиві показання» [34, с. 151].

Аналіз матеріалів судово-слідчої практики [Додаток Б] дав змогу зробити висновок, що одночасний допит раніше допитаних осіб проводився:

– між підозрюваним та потерпілим – у 91 % випадків;

– між підозрюваним та свідками – 2 %;

– між підозрюваними особами – у 7 %.

На основі опрацювання матеріалів кримінальних проваджень [Додаток Б] було встановлено, що у 63 % випадках під час проведення досліджуваної процесуальної дії між потерпілим та підозрюваним останній повністю або частково засвідчив свідчення, які раніше заперечував.

Також слід акцентувати увагу на тому, що поінформованість уповноваженої особи дає їй змогу здобути психологічну перевагу над правопорушником, що є запорукою успішності допиту та одночасного допиту раніше допитаних осіб. З'ясовано, що підозрювані у вчинені досліджуваної категорії протиправних діянь у більшості випадків мають високий рівень технічної підготовки, що переважає рівень знань про електронно-обчислювальну техніку уповноваженої особи, яка проводить допит. З огляду на це виняткове значення мають експертні висновки, які отримані за результатами дослідження виявлених доказів (електронної переписки, акаунтів, електронних операцій). Застосування визначених експертних досліджень, а також пред'явлення результатів проведення інших процесуальних дій надасть уповноваженій особі можливість подолати опір підозрюваного та підштовхувати його до визнання своєї вини.

Констатуючи вищенаведене, зазначимо, що подальший етап розслідування починається з моменту пред'явлення підозри. Встановлено, що при розслідуванні кримінальних правопорушень, пов'язаних з використанням

Інтернет-банкінгу, є ряд беззаперечно важливих дій, які необхідно швидко та ефективно реалізовувати. Серед них необхідно виокремлено допит підозрюваного для з'ясування механізму та обставин вчинення протиправного діяння, одночасний допит раніше допитаних осіб та обшук. Визначені процесуальні дії нами були опрацьовані та отримали певні тактичні рекомендації стосовно їх проведення. Зокрема, застосовуванні таких тактичних прийомів: створення уявлення про інформованість уповноваженої особи; швидкий темп допиту; використання фактора раптовості; створення напруги; пред'явлення речових доказів; застосування відеозапису. Також встановлено, що у 63 % випадках під час проведення одночасного допиту між потерпілим та підозрюваним останній повністю або частково засвідчив свідчення, які раніше заперечував.

3.3. Особливості використання спеціальних знань у кримінальному провадженні

Використання спеціальних знань є важливою складовою в кримінальних провадженнях будь-якої категорії. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, також характеризується тим, що без залучення відповідних спеціалістів окремі СРД, НСРД та інші процесуальні дії не можуть бути проведені ефективно. Тому дослідження вказаної наукової категорії є обов'язковим.

Доречною вважаємо судження Г. С. Бідняк вказує на те, 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» [10, с. 41–44].

А вже І. І. Когутич до основних процесуальних форм використання спеціальних знань долучає такі: «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» [59, с. 113–114].

Стосовно використання спеціальних знань ми поділяємо позицію В. В. Тіщенка, який виокремлює серед них такі категорії як-от: «…безпосередні, тобто такі, що прямо спрямовані на збирання й отримання доказів; опосередковані, тобто ті, що сприяють збиранню й оцінці доказів» [156, с. 351-352].

Вважаємо вірною думку Л. Ш. Мамедової, яка наголосила, що при розслідуванні кіберзлочинів варто 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) в досліджуваній категорії кримінальних проваджень. Крім того, авторка зауважила, що з метою ефективного розслідування та розкриття зазначеної категорії

протиправних діянь доцільно приділити увагу підвищенню кваліфікації експертів і спеціалістів, створити передумови для впровадження єдиної системи підготовки та підвищення кваліфікації кадрів, які залучаються до протидії кіберзлочинності [90, с. 394].

Окрема група науковців (К. О. Чаплинський, Н. В. Павлова, Д. А. Птушкін) доцільно наголошує на тому, 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» [102, с. 135].

А вже С. С. Чернявський виокремив та проаналізував наступні форми застосовування спеціальних знань у справах про фінансове шахрайство, як-от: «…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 %)» [165, с. 19].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] було визначено, що спеціаліст у більшості випадків залучався до проведення наступних процесуальних дій:

– огляд місця події (100 %);

– огляд електронної інформації (100 %);

– обшук (98 %);

– тимчасовий доступ до речей та документів (51 %);

– допит (41 %);

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

Вірною вбачаємо думку О. О. Волобуєвої, яка вказувала на те, що «…першорядною, найбільш важливою та складною формою використання спеціальних знань є участь спеціаліста у проведенні СРД. Це пояснюється тим, що в цьому випадку діяльність спеціаліста спрямовано на пошук (сприяння в пошуку) речових доказів (слідів, предметів і об'єктів) – джерел інформації про скоєний злочин, наявність яких є базисом у відтворенні слідчим обставин злочинної події та побудові алгоритму дій, спрямованих на розкриття та розслідування злочину. Крім того, саме від результативності слідчої дії залежить необхідність реалізації інформаційно-доказового потенціалу виявлених речових доказів за допомогою проведення експертних досліджень» [20, с. 34].

В свою чергу, Т. В. Коршикова наголошує на важливості ролі спеціаліста у наданні консультацій уповноваженій особі під час розслідування шахрайств, що вчиняються з використанням ЕОТ. Зокрема, авторка до предмету консультацій зі спеціалістом у галузі комп'ютерних технологій відносить наступні питання: «…а) визначення способу та механізму використання ЕОТ під час вчинення шахрайства; б) з'ясування ступеня належності того чи іншого предмета, який належить до ЕОТ, в механізмі вчинення шахрайства; в) способи використання ЕОТ у механізмі вчинення шахрайства; г) порядок збереження вилучених ЕОТ; д) можливість використання певного виду технічних засобів для вчинення шахрайства» [64, с. 183].

Запропоновано застосовування спеціальних знань у формі залучення спеціаліста відповідного профілю при його безпосередньої участі у процесуальних діях, зокрема:

1) огляду комп'ютерної техніки – спеціаліст в галузі комп'ютерних

технологій для ефективного виявлення та вилучення слідів правопорушення;

2) допиту потерпілого – спеціаліста-фоноскопіста для роботи з голосовими даними (запис розмови потерпілого та злочинця), які є в матеріалах кримінального провадження, а також подальшого призначення та проведення відповідних експертиз;

3) обшуку – спеціаліст в галузі комп'ютерних технологій для ефективного вилучення електронно-обчислювальної техніки та носіїв інформації шляхом якісного подолання систем захисту, роботи з пристроями електроживлення, а також правильного зняття цифрових даних.

Для прикладу, 28.06.2022, о 20 годині 07 хвилин, гр. І. перебував у заздалегідь орендованій квартири, використовуючи систему призначену для дистанційного керування банківськими рахунками банку «Приватбанк» веб-сторінку інтернет-банкінгу «Приват24». Реалізуючи свій злочинний умисел направлений на несанкціоноване втручання в роботу інформаційних (автоматизованих) систем, використовуючи мобільний телефон марки «IPhone», із встановленим на ньому браузером «Файерфокс», з доступом до мережі Інтернет, отримав від невстановленої особи фінансовий номер телефону і пароль клієнта АТ КБ «Приватбанк» гр. А., та у полях вводу відповідних даних на веб-сторінці інтернет-банкінгу «Приват24» особисто ввів фінансовий номер телефону і пароль доступу потерпілого, а також перейшов до особистого кабінету вищевказаного клієнта, чим несанкціоновано втрутився у роботу автоматизованої системі ПАТ КБ Приватбанк інтернет-банкінгу «Приват24». Таким чином, своїми незаконними діями правопорушник спотворив інформацію про належного користувача облікового запису, не маючи законного доступу до нього, з метою подальшого дистанційного керування вищевказаними картками, отримав можливість розпоряджатись коштами та функціями вищезазначеного банківського рахунку, а також отримав доступ до всіх послуг, які пропонує web-банкінг «Приват24», та змогу використовувати їх на власний розсуд [143]. В ході досудового розслідування мобільний телефон спеціаліст

в галузі комп'ютерних технологій було вилучено у підозрюваного, розблоковано і знято всю необхідну доказову інформацію.

Призначення експертиз є однією з найбільш розповсюджених слідчих (розшукових) дій під час розслідування більшості кримінальних правопорушень. Не є виключенням і протиправні діяння, пов'язані з використанням інтернет-банкінгу [140, с. 35].

З приводу призначення експертиз Є. І. Макаренко, О. В. Негодченко та В. М. Тертишник вказували, що вибір правильного моменту «…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» [87, с. 37].

Досить вдалим вбачається судження Ю. М. Чорноус, яка зазначила, 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» [169, с. 221].

Доречним в розрізі зазначеного вважаємо твердження І. О. Коваленка,

який зауважував, що XXI сторіччя можна впевнено назвати «комп'ютерним сторіччям». Автор відмітив, що стрімкий розвиток інформаційних технологій полегшив життя людства та, в свою чергу, породив нові кримінальні правопорушення в сфері інформаційних технологій. Крім того, дослідник акцентував увагу на тому, щоб провести платіж, у більшості випадків використовується Internet banking, пояснюючи це тим, що для цього не потрібно йти у відділення банку – це все можна зробити за декілька секунд, маючи доступ до Інтернету. Як висновок, науковець вказав на те, що незважаючи на масу переваг, ця ситуація активізувала спалах вчинення кримінальних правопорушень, кількість яких збільшуються щорічно [54, с. 262].

З приводу об'єктів експертного дослідження, то, наприклад, А. В. Реуцький запропонував наступний їх перелік: 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. [119, с. 14]. Повністю погоджуємося з наведеним переліком.

В свою чергу, О. В. Одерій та С. В. Самойлов вірно засвідчували, 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].

Зі свого боку, С. С. Чернявський наголосив на обов'язковому призначенні та проведенні судово-бухгалтерської, фінансово-економічної почеркознавчої експертиз, техніко-криміналістичної експертизи документів,

комп'ютерно-технічних експертиз. Автор визначив це як необхідну передумову подальшого удосконалення окремих методик розслідування фінансового шахрайства [165, с. 19].

А вже Б. Є. Лук'янчиков, Є. Д. Лук'янчиков та С. Ю. Петряєв зазначали, 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. Автори зауважили, що 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. Крім того, дослідники наголосили на тому, що 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 [85, с. 483].

Найбільш точною для предмету нашого дослідження вважаємо позицію Т. В. Коршикової, яка на базі опрацювання результатів кримінальних проваджень щодо шахрайств, що вчиняються з використанням ЕОТ, виокремила «…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)» [66, с. 297].

Доречною також вважаємо позицію А. Ф. Волобуєва, В. О. Малярової та Р. Л. Степанюка, які до засобів учинення протиправних діянь у сфері ЕОТ зараховують наступні: «…мережу та засоби стільникового зв'язку, глобальну світову телекомунікаційну мережу Інтернет, засоби комп'ютерної техніки, зокрема спеціальне програмне забезпечення, програми-віруси, програми-шкідники, периферійне обладнання (принтер, CD-ROM-накопичувач, стример), а також носії комп'ютерної інформації («флешки», диски) та засоби телефонного зв'язку. Окрім того, для вчинення шахрайств за допомогою пластикових кредитних карток злочинці можуть користуватися, відповідно, банкоматами, спеціально виготовленими пристроями для зчитування інформації з чужих карток, електронними терміналами, імпрінтерами та декодерами. Усі ці об'єкти можуть бути носіями тієї чи іншої інформації, яка має значення у кримінальному провадженні» [73, с. 162].

На основі проаналізованих кримінальних проваджень спробуємо визначити види судових експертиз, які потрібно призначати під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу:

– судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення);

– експертиза телекомунікаційних систем і засобів;

– судово-бухгалтерська експертиза.

Окрема група вчених-криміналістів головними завданнями судової експертизи комп'ютерних засобів окреслила наступні: «…визначення виду

(типу, марки) та властивостей апаратного засобу, а також його технічних і функціональних характеристик для вирішення певних функціональних завдань, установлення місця, ролі та функціонального призначення досліджуваного об’єкта в мережі; визначення фактичного стану та справності апаратного засобу й наявності фізичних дефектів, установлення причинного зв’язку між використанням конкретних можливостей апаратних засобів і результатами їх використання, визначення умов (обстановки) застосовування апаратних засобів, виявлення властивостей і характеристик мережі, встановлення її архітектури й конфігурації, виявлення встановлених мережних компонент та організація доступу до даних, визначення відповідності виявлених характеристик типовим для конкретного класу засобів мережної технології та ін. Під час цієї експертизи може здійснюватися ідентифікація конкретних апаратних засобів за встановленими загальними й окремими ознаками, наприклад серійні номери, формфактори, місткість і структура накопичувача, середній час доступу до даних, швидкість передання даних, спосіб і щільність магнітного запису та ін.» [73, с. 273].

Найбільш вірною стосовно визначення об’єктів та завдань комп’ютерно-технічного дослідження ми вважаємо позицію А. І. Кунтія. Автор серед перших визначив такі як-от: «…цифрові носії інформації (накопичувачі на гнучких і жорстких магнітних дисках, диски для лазерних систем зчитування, флеш-накопичувачі, картки пам’яті), комп’ютер загалом, його окремі блоки та пристрої, комп’ютерні комплекси, програмні продукти. До основних завдань експертизи комп’ютерної техніки та програмних продуктів належать: установлення робочого стану комп’ютерно-технічних засобів; установлення обставин, пов’язаних із 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» [71, с. 882-883].

На основі вивчення матеріалів кримінальних проваджень [Додаток А]

виокремлено об’єкти, що направляються на експертизу:

– власні ґаджети потерпілого (смартфон, планшет, ноутбук, комп’ютер, модеми, маршрутизатори);

– власні ґаджети підозрюваного (смартфон, планшет, ноутбук, комп’ютер, модеми, маршрутизатори);

– флеш-накопичувачі;

– жорсткі диски та ін.

А вже О. І. Коваленко акцентує увагу на тому, що «…існують такі розповсюджені способи підміни реальної IP-адреси: підключення до проксі-серверу, використання інтернет-браузера TOR, маскування IP-адреси через VPN. Під час КМЕ 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» [57, с. 165].

Також вбачаємо потребу наголосити на необхідності професійної підготовки майбутніх працівників правоохоронних органів. В розрізі зазначеного, І. В. Пиріг говорить про те, що «…відсутність зацікавленості у використанні своїх знань, тобто функціонального компоненту, призводить до зниження гносеологічного та нормативного – зникає бажання підвищувати рівень своїх спеціальних і юридичних знань. Звідси з’являється плинність кадрів, особливо серед випускників вищих навчальних закладів МВС. За даними Донецького юридичного інституту, серед випускників, що закінчили експертний факультет, кожний п’ятий звільняється протягом першого року професійної діяльності. Молоді спеціалісти з юридичною освітою та певними знаннями в галузі техніки знаходять їх застосування в інших галузях

промисловості та бізнесу» [105, с. 83].

В свою чергу, окремі автори наголошують на тому, що для опрацювання відомостей, які розміщаються на комп'ютерних носіях «…експерту надається сам комп'ютерний носій, а за потреби комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій). Для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях. Системні блоки персональних комп'ютерів надаються в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блока до мережі живлення. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду. Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них. З метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки» [60].

Підсумовуючи, зазначимо, що призначення експертиз є однією з найбільш розповсюджених слідчих (розшукових) дій під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Визначено види судових експертиз, які потрібно призначати в кримінальних провадженнях досліджуваної категорії.

Висновки до розділу 3

Після опрацювання тактики проведення процесуальних дій при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, необхідно зробити такі висновки:

1. Визначено особливості початкового етапу розслідування та

охарактеризовано специфіку організаційних заходів та процесуальних дій. На основі аналізу наукових праць вчених (А. І. Кунтій, Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) сформульовано криміналістичні версії, які можна висувати на початковому етапі розслідування.

2. На основі вивчення матеріалів кримінальних проваджень виокремлено найбільш поширені процесуальні дії початкового етапу розслідування досліджуваної категорії протиправних діянь, а саме: огляд місця події (98 %), огляд електронної інформації (94 %), обшук (91 %), призначення та проведення експертиз (100 %), тимчасовий доступ до речей і документів (79 %), огляд документів (53 %), допит потерпілих та свідків (100 %).

3. Встановлено місця, які найчастіше підлягають огляду на початковому етапі розслідування, зокрема: робоче місце потерпілого, робоче місце підозрюваного, банкомати, місця доступу до загальної мережі Wi-Fi та ін. З'ясовано, що на початковому етапі розслідування необхідно максимально забезпечити збереження інформації, яка перебуває на флеш-накопичувачах, жорстких дисках (носіях), кеш-пам'яті відповідного пристрою, в хмарних сховищах та ін. Для цього обов'язково потрібно застосовувати проведення одночасних обшуків за різними адресами ймовірного знаходження правопорушників. Встановлено особливості вилучення заблокованих та розблокованих переносних ґаджетів (смартфон, smart-годинник, портативний відео-реєстратор, GPS-навігатор).

4. Означено перелік об'єктів, що повинні вилучатись під час обшуку в досліджуваній категорії кримінальних проваджень. Для визначення місць перебування вказаних осіб необхідно організувати та провести низку НСРД, серед яких виділено спостереження за об'єктом та прослуховування телефонних переговорів. Підкреслено важливість детального огляду смартфонів, сітьового та серверного обладнання, комп'ютерної техніки, а також її комплектуючих (процесорів, модулів пам'яті, жорстких дисків).

5. Встановлено, що до проведення допиту потерпілих необхідно

оглянути наявну в них електронно-обчислювальну техніку (смартфони, ноутбуки, планшети), за допомогою якої відбувалася переписка чи розмова з правопорушником. Зосереджено увагу на *допиті потерпілого* й *свідка*. Визначено основні завдання допиту, а також сформовано перелік об'єктів, що варто демонструвати під час допиту потерпілого або свідка.

6. З'ясовано, що на подальшому етапі розслідування переважно проводяться такі слідчі (розшукові) дії: допит підозрюваних (100 %), одночасний допит раніше допитаних осіб (82 %), призначення та проведення експертиз (100 %), пред'явлення для впізнання за голосом (3 %) та в натурі (1 %). Наголошено на обов'язковому проведенні пред'явлення підозрюваного для впізнання у випадках можливості встановлення потерпілим його тотожності за голосом (у випадках телефонної розмови) або в натурі (у випадках розмови за допомогою відео-конференції). Особливу увагу приділено тактиці допиту підозрюваного. З'ясовано, що під час допиту підозрюваних необхідно встановлювати наступні факти: електронно-обчислювальна техніка, яка була застосована для вчинення протиправних діянь; програмне забезпечення, яке використовувалось для вчинення кримінального правопорушення (програми віддаленого доступу, «трояни», «боти»); логіни та паролі акаунтів, які використовувались для спілкування з потерпілими; реквізити банківських карт та рахунків, на які переказувались кошти.

7. Визначено безконфліктні й конфліктні ситуації допиту. Охарактеризовано тактичні прийоми, що найчастіше застосовуються під час допиту підозрюваного: створення уявлення про інформованість уповноваженої особи – 89 %, швидкий темп допиту – 56 %, використання фактора раптовості – 57 %, створення напруги – 69 %, пред'явлення речових доказів – 33 %, застосування відеозапису – 45 %. Серед них особливе місце займає пред'явлення речових доказів. Висвітлено особливості залучення до проведення допиту різних спеціалістів, серед яких виділено фахівців у економічній кібернетиці, цифрових технологіях, компетентною у галузі

комерційної чи банківської діяльності. З'ясовано, що для усунення розбіжностей у показаннях потерпілих, свідків та підозрюваних у 23 % випадках здійснювався одночасний допит двох або більше раніше допитаних осіб. Одночасний допит раніше допитаних осіб проводився: між підозрюваним та потерпілим – у 91 % випадків, між підозрюваним та свідками – 2 %, між підозрюваними особами – 7 %.

8. Розглянуто поняття, форми, види й суб'єкти використання спеціальних знань та участь спеціаліста під час проведення слідчих (розшукових) дій. Визначено, що спеціаліст у більшості випадків залучався до проведення наступних процесуальних дій: огляд місця події (100 %), огляд електронної інформації (100 %), обшук (98 %), тимчасовий доступ до речей та документів (51 %), допит (41 %), зняття інформації з транспортних телекомунікаційних мереж та електронних систем (100 %). Охарактеризовано процесуальні та непроцесуальні форми використання спеціальних знань у кримінальному провадженні.

9. На підставі аналізу судово-слідчої практики визначено перелік судових експертиз, що можуть призначатися при розслідуванні кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу: а) судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів, експертиза даних, експертиза програмного забезпечення); б) експертиза телекомунікаційних систем і засобів; в) судово-бухгалтерська експертиза. З'ясовано особливості підготовки і проведення судових експертиз. Виокремлено об'єкти, що направляються на експертизу: власні ґаджети потерпілого (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори), власні ґаджети підозрюваного (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори), флеш-накопичувачі, жорсткі диски та ін.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, що виявляється в розробленні теоретичних і практичних засад методики розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, а також формулювання науково обґрунтованих пропозицій і практичних рекомендацій щодо їх розвитку й удосконалення з урахуванням досвіду зарубіжних країн. В результаті дослідження сформовано низку теоретичних положень, висновків і практичних рекомендацій, основними з яких є такі:

1. Здійснено криміналістичний аналіз функціонування сфери використання банківських електронних платежів (е-банкінгу). Виокремлено основні фактори, що зумовлюють учинення протиправних дій. Здійснено аналіз наукових поглядів учених стосовно кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу. З’ясовано, що низка вітчизняних і зарубіжних дослідників (Д. Деннінг, О. Довженко, Г. Загіка, В. Клей, О. Порфімович, Ф. Уільямс, О. Чернавський, Л. Шеллі) досліджували питання визначення сутності кіберзлочинності, а також можливі способи протидії та напрями запобігання вказаному негативному явищу. Проте кількість звернень за фактами протиправних дій дедалі зростає, злочинна діяльність набуває все більш латентного та організованого характеру. Заходи щодо протидії злочинним проявам з урахуванням запровадженого воєнного стану не відповідають сучасним загрозам і потребують удосконалення.

Запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь, зокрема: 1) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у сфері власності; 2) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у сфері господарської діяльності; 3) кримінальні правопорушення, пов’язані із використанням інтернет-банкінгу, у сфері використання

електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

2. Визначено сучасні наукові підходи до розуміння криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та основних її елементів, на підставі чого окреслено кореляційні зв'язки між ними. Система криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, складається з таких елементів: спосіб і обстановка вчинення правопорушення, слідова картина, особа злочинця та особа потерпілого.

Запропоновано авторське визначення. Доведено, що правильно сформована структура криміналістичної характеристики дозволить виокремити найбільш чіткі кореляційні зв'язки, які допоможуть як в побудові криміналістичних версій, так і ефективному проведенні окремих слідчих (розшукових) дій та НСРД.

3. Охарактеризовано окремі елементи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Способи досліджуваної категорії протиправних діянь мають глибокі грані, які виявляються у сукупності взаємопов'язаних дій з підготовки, безпосереднього вчинення та їх приховування. Дані стосовно вказаних способів є найбільш інформативним джерелом у кримінальному провадженні.

Охарактеризовано типові способи вчинення досліджуваної категорії кримінальних правопорушень: 1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг); 2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима,

обладнанням для їх виготовлення; 4) розповсюдження шкідливих програмних чи технічних засобів або їх збут з використанням мережі Інтернет; 5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах; 6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін. Визначено способи підготовки та приховування протиправних діянь. З'ясовано злочинні схеми, що застосовуються під час запровадженого воєнного стану.

Визначено обстановку протиправних дій, яка характеризується обставинами місця та часу, що в більшості випадків є невизначеними, адже обіймають велику кількість об'єктів, що можуть бути місцем події.

Охарактеризовано місця учинення досліджуваної категорії кримінальних правопорушень: місця розташування електронно-обчислювальної техніки, з якої вчинились протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 61 %; місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %; місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу – 12 %.

Встановлено слідову картину кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Визначено, що досліджувані категорії протиправних діянь характерні електронні сліди (віртуальні, цифрові, комп'ютерні). Зазначені сліди переважно знаходяться в наступних місцях: акаунти, пам'ять електронно-обчислювальної техніки, профілі соціальних мереж, сайти для криптовалютних переписок, бази даних операторів зв'язку та інтернет-провайдерів, флеш-носії.

Узагальнено криміналістично вагомі ознаки особи злочинця, на підставі чого сформовано ймовірний «портрет» правопорушника. Вирізнено віктимогенні групи осіб щодо яких було вчинено кримінальні правопорушення визначеної категорії.

4. Визначено особливості криміналістичного аналізу первісної інформації та охарактеризовано основні напрями організації розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу.

Окреслено коло обставин, які підлягають встановленню: 1) обставини, що характеризують вчинення кримінальних правопорушень, пов’язаних з використанням інтернет-банкінгу: а) відомості про час, місце та спосіб учинення протиправних дій, як-от, застосовування шкідливих програм чи вірусів, заведених до комп’ютерного забезпечення потерпілого та дублювання за допомогою них акаунту на власний ґаджет (смартфон, планшет, ноутбук, комп’ютер); б) відомості про віртуальні сліди кримінального правопорушення; в) встановлення місця одержання безпідставного доступу до мережі Інтернет; г) засоби, які застосовувалися під час скоєння протиправного діяння (технічні – різні ґаджети, зокрема, смартфони, ноутбуки, модеми; програмні – шпигунські програми, браузери, шкідливі віруси); 2) обставини, які розкривають особу правопорушника з різних сторін (професійної, злочинної. розумової); 3) обставини, які розкривають особу потерпілого з різних сторін (професійної, злочинної. розумової); 4) причинно-наслідкові взаємозв’язки: факт чіткого зв’язку між діями правопорушників та їх наслідками; 5) обставини, які обтяжують чи пом’якшують покарання, або у цілому виключають кримінальну відповідальність за скоєння протиправних діянь, пов’язаних із використанням інтернет-банкінгу.

5. Конкретизовано слідчі ситуації, що виникають на початковому етапі розслідування, а також відповідні кожній з них алгоритми дій працівників правоохоронних органів. Серед типових слідчих ситуацій виокремлено наступні: 1) скоєно кримінальне правопорушення, пов’язане з використанням інтернет-банкінгу, має місце достатня доказова база, особу правопорушника встановлено – 6 %; 2) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника не встановлено – 64 %; 3) скоєно

протиправне діяння, має місце достатня доказова база, особу правопорушника встановлено, та протиправні дії приховані під легальну фінансову діяльність – 9 %; 4) скоєно протиправне діяння, має місце заява потерпілого, відсутня будь-яка доказова база – 21 %.

Для вирішення вказаних слідчих ситуацій запропоновано вирішення наступних тактичних завдань: 1) з'ясування механізму кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу; 2) визначення точок доступу, з яких реалізувалися протиправні дії; 3) перевірка цифрових слідів, які залишені під час проведення електронних операцій; 4) встановлення осіб, які реалізували незаконне втручання в роботу інтернет-банкінгу; 5) перевірка мобільних контактів правопорушника та його особистих зв'язків; 6) перевірка банківських і поштових переказів правопорушника; 7) з'ясування всіх епізодів протиправної діяльності; 8) вжиття заходів стосовно попередження протидії розслідуванню.

6. Визначено особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Сформульовано криміналістичні версії, які можна висувати на початковому етапі кримінального провадження. Конкретизовано організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій.

Визначено тактику огляду. Виокремлено вузлові ділянки, де можуть бути зосереджені сліди протиправних дій: робоче місце потерпілого, робоче місце підозрюваного, банкомати, місця доступу до загальної мережі Wi-Fi.

Розкрито організаційно-підготовчі заходи і тактику обшуку. Окреслено перелік об'єктів, які необхідно вилучати під час обшуку: 1) електронно-обчислювальна техніка, за допомогою якої здійснювалось втручання в роботу інтернет-мереж для їх дестабілізації або отримання відомостей, необхідних для реалізації операцій в інтернет-банкінгу (комп'ютери, планшети, ноутбуки, смартфони); 2) реквізити карток, що викрадені з серверів магазинів електронної торгівлі, платіжних і

розрахункових систем, з персональних ґаджетів користувачів; 3) фотографії, відеозаписи, на яких наявні дані, що мають значення для кримінального провадження; 4) квитанції про здійснення банківських операцій; 5) смартфони або інші ґаджети, в яких наявна адресна книга (ПІБ й адреси клієнтів фінансових установ, підприємств та організацій різних форм власності); 6) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб та ін.

Значну увагу присвячено тактиці проведення окремих НСРД, зокрема, спостереження за об'єктом та прослуховування телефонних переговорів.

Зосереджено увагу на допиті потерпілого та окреслено основні його завдання: з'ясувати обставини вчинення протиправного діяння (час, місце, зокрема, з доступом до загальної мережі Wi-Fi, наявність поблизу сторонніх осіб – можливість віддаленого підключення з іншого ґаджету); проаналізувати його передумови (чи були надіслані на номер потерпілого та прийняті повідомлення – в якому месенджері та якого змісту, чи були наявні дзвінки – в якому месенджері та якого змісту); встановити послідовність дій потерпілого після вчинення кримінального правопорушення (одразу повідомив в правоохоронні органи чи своїм знайомим, родичам, що зробив з ґаджетом – вимкнув, перезавантажив, продовжив користуватися). Визначено, що під час допиту потерпілого або свідка доцільно демонструвати певні об'єкти: а) скріншоти повідомлень переписки зі злочинцем; б) зображення (скріншот) документу, який підтверджує зняття коштів з рахунку потерпілого; в) виписку з банківського рахунку потерпілого; г) у випадках розмови зі злочинцем в телефонному режимі чи в режимі відео-конференції з'ясувати у потерпілого чи зробив він її запис – якщо так, то долучити до кримінального провадження для подальшого використання під час проведення пред'явлення для впізнання.

7. Охарактеризовано подальший етап розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Встановлено, що на даному етапі розслідування, як правило, визначене коло

підозрюваних, тому характерного значення набувають заходи щодо подолання їхньої протидії під час проведення слідчих (розшукових) дій.

Наголошено на обов'язковому проведенні пред'явлення підозрюваного для впізнання.

Визначено безконфліктні й конфліктні ситуації *допиту підозрюваного*. З'ясовано, що для вирішення конфліктних ситуацій застосовуються різноманітні тактичні прийоми допиту. Найбільш ефективним серед них вказано пред'явлення речових доказів, серед яких можуть демонструватись наступні об'єкти: свідчення потерпілих; протоколи пред'явлення для впізнання з позитивним результатом (підозрюваного впізнано за голосом чи в натурі); флеш-накопичувачі та жорсткі диски з інформацією про банківські операції з грошовими коштами; скріншоти хмарних сховищ; скріншоти переписки з потерпілими.

Розкрито тактику проведення одночасного допиту двох або більше раніше допитаних осіб.

Акцентується увага на тому, що поінформованість уповноваженої особи дає їй змогу здобути психологічну перевагу над правопорушником, що є запорукою успішності допиту та одночасного допиту раніше допитаних осіб. З'ясовано, що підозрювані у вчинені досліджуваної категорії протиправних діянь у більшості випадків мають високий рівень технічної підготовки, що переважає рівень знань про електронно-обчислювальну техніку уповноваженої особи, яка проводить допит. З огляду на це виняткове значення мають експертні висновки, які отримані за результатами дослідження виявлених доказів (електронної переписки, акаунтів, електронних операцій). Застосування визначених експертних досліджень, а також пред'явлення результатів проведення інших процесуальних дій надасть уповноваженій особі можливість подолати опір підозрюваного та підштовхувати його до визнання своєї вини.

8. Виокремлено особливості використання спеціальних знань під час розслідування кримінальних правопорушень, пов'язаних із використанням

інтернет-банкінгу.

Виділено найбільш поширені форми використання спеціальних знань: використання консультативної допомоги спеціаліста (91 %), призначення і проведення судових експертиз (100 %), участь спеціаліста при проведенні слідчих (розшукових) дій (89 %).

Запропоновано застосовування спеціальних знань у формі залучення спеціаліста відповідного профілю при його безпосередньої участі у процесуальних діях, зокрема: 1) огляду комп'ютерної техніки – спеціаліст в галузі комп'ютерних технологій для ефективного виявлення та вилучення слідів правопорушення; 2) допиту потерпілого – спеціаліста-фоноскопіста для роботи з голосовими даними (запис розмови потерпілого та злочинця), які є в матеріалах кримінального провадження, а також подальшого призначення та проведення відповідних експертиз; 3) обшуку – спеціаліст в галузі комп'ютерних технологій для ефективного вилучення електронно-обчислювальної техніки та носіїв інформації шляхом якісного подолання систем захисту, роботи з пристроями електроживлення, а також правильного зняття цифрових даних.

Наголошено на призначенні судових експертиз при розслідуванні досліджуваної категорії протиправних діянь.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Александров Ю. В., Гель А. П., Семаков Г. С. Кримінологія : Курс лекцій. Київ : МАУП, 2002. 296 с.

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

3. Антонюк О. А. Наукові диспути стосовно профілактики під час розслідування кримінальних правопорушень проти громадського порядку. *Науковий вісник публічного та приватного права*. 2018. Випуск № 2. Том 2. С. 177–182.

4. Апопій В. В. Інтернет-торгівля : проблеми і перспективи розвитку. *Регіональна економіка*. 2003. № 1. С. 25–32.

5. Ахтирська Н. М. Актуальні проблеми розслідування кіберзлочинів : навчальний посібник. Київ : ВПЦ «Київський університет», 2018. 229 с

6. Баланюк О. В. Підготовка до злочину : поняття та криміналістична класифікація. *Актуальні проблеми держави і права*. 2006. С. 192–196.

7. Бахін В. П., Лук'янчиков Б. Є. Склад і призначення криміналістичної характеристики злочинів. *Правничий часопис Донецького університету*. 2000. № 1 (4). С. 39–43.

8. Бедь В. В. Юридична психологія : навчальний посібник. Київ : «Каравелла»; Львів : «Новий світ-2000», «Магнолі плюс», 2003. 376 с.

9. Берназ В.Д. Криміналістична характеристика як наукова категорія. *Південноукраїнський правничий часопис*. №1. 2006. С. 16–18.

10. Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монограф. Дніпро : Дніпроп. держ. ун-т внутр.

справ, 2019. 152 с.

11. Біленчук П. Д., Перкін В. І. Тактичні прийоми, тактичні комбінації та тактичні операції в розслідуванні злочинів : навчальний посібник. Київ : Українська академія внутрішніх справ, 1996. 32 с.

12. 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.

13. Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : автореф дис... канд. юрид. наук : 12.00.09. Національна юридична академія України імені Ярослава Мудрого. Харків, 2002. 16 с.

14. Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : дис... канд. юрид. наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2002. 218 с.

15. Весельський В. К. Слідча ситуація як категорія криміналістичної тактики. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 193–199.

16. 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.

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

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

19. Волобуєв А. Ф. Профілактична діяльність слідчого при розслідуванні злочинів : Лекція для всіх форм навчання. Харків :

Національний університет внутрішніх справ, 2003. 23 с.

20. Волобуєва О. О. Взаємодія слідчого з фахівцями під час збору інформації про особу, що скоїла злочин : дис. ... канд. юрид. наук : 12.00.09 / Київський національний ун-т внутрішніх справ. Київ, 2006. 236 с.

21. Головко Н. І. Соціальна профілактика правопорушень : навч. посібник. Київ : ДП «Видавничий дім «Персонал», 2017. 174 с.

22. Директива кібербезпеки NIS 2. URL : https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua#:~:text=NIS%20(the%20security%20of%20network,пошуковиків%20і%20сервісів%20хмарних%20обчислень). (дата звернення – 15.05.2023).

23. Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 19–22.

24. Довженко О. Ю. Основи методики розслідування кіберзлочинів : автореф. дис. … к-та юр. наук : 12.00.09. Харківський національний університет внутрішніх справ. Харків, 2020. 18 с.

25. Довженко О. Ю. Основи методики розслідування кіберзлочинів : дис. … к-та юр. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2020. 229 с.

26. Довженко О. Ю. Поняття кіберзлочину з криміналістичної позиції. *Юридичний вісник*. 2018. № 3. С. 79–83.

27. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи : підписаний в м. Страсбург 28 січня 2003 року. URL : http://zakon0.rada.gov.ua/laws/show/994_687 (дата звернення – 06.02.2023).

28. Дрозд В. Г. Запровадження міжнародно-правових стандартів захисту прав людини у світлі реформування кримінального процесуального законодавства. *Вісник ЛДУВС ім. Е.О. Дідоренка.* 2017. № 4 (80). С. 58–68.

29. Дрозд В. Г. Правове регулювання досудового розслідування: проблеми теорії та практики : монографія. Одеса : Видавничий дім

«Гельветика», 2018. 448 с.

30. Дрозд В. Г. Судова практика щодо допустимості доказів, отриманих у результаті проведення негласних слідчих (розшукових) дій. *Підприємництво, господарство і право*. 2020. № 9. С. 185–190.

31. Дрозд В. Г. Сутність досудового розслідування як стадії кримінального провадження. *Наука і правоохоронна діяльність*. 2017. № 3 (37). С. 185–190.

32. Дуда Х. І. Поняття комп'ютерних слідів злочину. *Науковий вісник Національного університету біоресурсів і природокористування України.* 2014. Вип. 197. Ч. 1. С. 262–267.

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

34. Єфімов М. М., Павлова Н. В., Чучко С. В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу Інтернет : теоретичні та праксеологічні засади : монографія. Одеса : Видавничий дім «Гельветика», 2022. 200 с.

35. 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.

36. Єфімов М. М., Чаплинський К. О. Профілактична діяльність уповноважених осіб як елемент методики розслідування кримінальних правопорушень проти моральності. *Міжнародна та правова безпека : теоретичні і прикладні аспекти :* матеріали V Міжнародної науково-практичної конференції (м. Дніпро, 12 березня 2021 р.). Дніпро: Дніпропетровський державний університет внутрішніх справ, 2021. С. 275–276.

37. Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020.

№ 2. Том 2. С. 141–148.

38. 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.

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

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

41. Зав'ялов С. М. Спосіб вчинення злочину : сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. … канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ України. Київ, 2005. 231 с.

42. Загіка Г. В. Кримінологічна характеристика комп'ютерної злочинності. *Правова держава*. 2002. № 4. С. 56–61.

43. 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.

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

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

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

47. Іщенко А. В. Фундаментальні та прикладні криміналістичні категорії. *Актуальні проблеми розкриття та розслідування злочинів у*

сучасних умовах : Міжнародна науково-практична конференція 5 листопада 2010 р., м. Запоріжжя : матеріали у 3 част. Запоріжжя. 2010. ч. 1. С. 180–182.

48. Іщенко А., Щербаков Г. Проблема слідчих ситуацій, як складова навчального курсу криміналістики. *Вісник Одеського інституту внутрішніх справ*. 2003. № 2. С. 57–63.

49. Кальман О. Г. Злочинність у сфері економіки України : теоретичні та прикладні проблеми попередження : дис. … д-ра юрид. наук : 12.00.08 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2004. 430 с.

50. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан]; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL : law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення – 07.05.2023).

51. Кіберзлочинність та кіберконфлікти : США. URL: https://www.tadviser.ru/index.php/Статья:Киберпреступность_и_кибероконфликты_:_США#2004:_.D0.9A.D0.B8.D1.82.D0.B0.D0.B9.D1.86.D1.8B_.D0.B0.D1.82.D0.B0.D0.BA.D1.83.D1.8E.D1.82_Lockheed-Martin (дата звернення – 18.03.2023).

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

53. 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.

54. 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.

55. 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: ДДУВС, 2021. С. 145–147.

56. 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.

57. 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.

58. Когутич І. І. Криміналістика : підручник. Київ : Атіка, 2008. 466 с.

59. 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.

60. Комп'ютерно-технічна експертиза. URL : https://www.hniise.gov.ua/13973-kompyuterno-texnchna-ekspertiza.html (дата звернення – 14.05.2023)

61. Конвенція про кіберзлочинність : підписана в м. Будапешт 23 листопада 2001 року. URL : http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення – 06.02.2023).

62. Корнієнко В. В., Стреляний В. І. Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування : методичні рекомендації. Харківський національний університет внутрішніх справ : Харків, 2015. 71 с.

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

64. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … канд. юрид.наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2021. 255 с.

65. 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.

66. 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.

67. Кочнєва А. О. Криміналістична методика розслідування злочинів: сучасний стан і проблеми розвитку. *Юридичний вісник*. 2016. № 1 (38). С. 157–161.

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

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

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

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

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

73. 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.

74. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/page#Text (дата звернення – 12.03.2023).

75. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення – 23.04.2023).

76. Кримінологія : Загальна та особлива частини : підруч. для студ. юрид. спец. вищ. навч. закл. / За заг. ред. І. М. Даньшина. Харків : Право, 2003. 422 с.

77. Кримінологія : підруч. для студ. вищ. навч. закл. / За заг. ред. О. М. Джужи. Київ : Юрінком Інтер, 2002. 378 с.

78. Кришевич О. В. Шахрайство у сфері обігу банківських платіжних карток: кримінально-правовий аспект. *Актуальні проблеми кримінального права:* матеріали X Всеукр. наук.-теоретичної конф. (Київ, 22 листоп. 2019 р.). Присвячено пам’яті професора П. П. Михайленка. Київ: Нац. акад. внутр. справ, 2021. С. 81–84.

79. Курман О. В. Способи несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. *Право і суспільство.* 2017. № 4. С. 245–249.

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

81. Лисенко В. В. Криміналістичне забезпечення діяльності податкової міліції (Теорія та практика) : монографія. Київ : Логос, 2004. 324 с.

82. Лисенко В. В. Проблеми криміналістичного забезпечення розслідування податкових злочинів : автореф. дис. … д-ра юрид. наук : 12.00.09 / Київ. нац. ун-т внутр. справ України. Київ, 2006. 33 с.

83. 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. (Запоріжжя, 5 листоп. 2010 р.). у 2-х ч. Ч. 1. Запоріжжя: ЗЮІ ДДУВС. 2010. С. 115–118.

84. 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.

85. 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.

86. Лускатов О. В. Теорія та практика розслідування нерозкритих злочинів минулих років : монографія. Дніпропетровськ, 2008. 192 с.

87. 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.

88. Малюга В. Структура методики розслідування окремих видів злочинів і місце в ній взаємодії слідчого. *Підприємництво, господарство і право*. 2015. № 8. С. 61–65.

89. Малярова В. О. Криміналістична методика: питання співвідношення криміналістичної характеристики з іншими. *Науковий вісник Ужгородського національного університету*. 2015. Серія Право. Випуск 35. Частина 1. Том 3. С. 111–113.

90. 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 – 23.04.2023).

91. Матусовский Г. А. Структура криміналістичної характеристики

злочинів. Криміналістика : Криміналістична тактика і методика розслідування злочинів. За ред. В. Ю. Шепітька. Харків : Право, 1998. 368 с.

92. Михайлов О. Є., Горбань А. В., Міщук В. В. Кримінологія : навч. посіб. Київ : Знання, 2012. 565 с.

93. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. канд. юрид. наук : 12.00.09. Академія праці і соціальних відносин Федерації профспілок України. Київ, 2005. 21 с.

94. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. канд. юрид. наук : 12.00.09 / Академія праці і соціальних відносин Федерації профспілок України. Київ, 2005. 220 с.

95. Мотлях О. І. Проведення обшуків та виїмок при розслідуванні злочинів, пов'язаних зі сферою комп'ютерних технологій. *Прокуратура Людина Держава*. 2005. № 1 (43). С. 57–67.

96. Мусієнко О. Л. Спосіб шахрайства як структурний елемент криміналістичної характеристики. *Науковий вісник Херсонського державного університету.* 2013. Випуск 4. Том 2. С. 151–153.

97. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

98. Охрімчук Т. В. Криміналістична характеристика шахрайства з фінансовими ресурсами. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Науково-практичний журнал. 2010. № 23. С. 369–374.

99. Охрімчук Т. В. Порушення кримінальної справи та планування розслідування шахрайства з фінансовими ресурсами. *Засади кримінального судочинства та їх реалізація в законотворчій і право застосовній діяльності* : наук.-практ. конф., 3 квітня 2009 року : тези допов. і повідомл. Київ, Атіка, 2009. С. 680–684.

100. Охрімчук Т. В. Способи вчинення шахрайства з фінансовими

ресурсами. *Правова держава : історія, сучасність та перспективи формування в Україні* : ІІІ Всеукраїнська наук.-практ. конф., 23 квітня 2010 року : матеріали. Запоріжжя : Юридичний ін-т ДДУВС, 2010. Ч.ІІ. С. 94–96.

101. 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.

102. Павлова Н. В., Птушкін Д. А., Чаплинський К. О. Теоретичні засади методики розслідування шахрайства, пов’язаного з відчуженням об’єктів нерухомого майна громадян: монографія. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2019. 206 с.

103. Павлова Н. В. Розслідування шахрайства при укладанні цивільно-правових угод щодо відчуження житла : монографія. Дніпропетровськ : Дніпропетровський державний університет внутрішніх справ, 2008. 176 с.

104. Піцик Ю. М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету.* 2017. № 26. С. 105–107.

105. Пиріг І. В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування : монографія. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2015. 432 с.

106. Плетенець В. М. Можливості використання фактору раптовості в умовах протидії розслідуванню. *Вісник ЛДУВС ім. Е. О. Дідоренка*. 2020. Вип. 2 (90). С. 239–247.

107. Події з історії кібербезпеки за 50 років. URL : https://datami.ua/podiyi-z-istoriyi-kiberbezpeki-za-50-rokiv/ (дата звернення – 18.03.2023).

108. Порфімович О. Л. Віртуальний криміналітет : від хакера до терориста (портрет явища). URL : http://journlib.univ.kiev.ua/index.php?act=article&article=2403 (дата

звернення – 30.05.2023).

109. Про електронну комерцію : Закон України від 3 вересня 2015 року № 675-VIII. *Офіційний вісник України*. 2015. № 78. Ст. 2590. URL : https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення – 09.03.2023).

110. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : Наказ Генеральної прокуратури від 30.06.2020 № 298. URL : https://zakon.rada.gov.ua/laws/show/v0298905-20#Text (дата звернення – 25.04.2023).

111. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 липня 1994 року № 80/94-ВР. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення – 09.03.2023).

112. Про Національний координаційний центр кібербезпеки : Указ Президента України від 7 червня 2016 року № 242/2016. *Офіційний вісник України*. 2016. № 46. Ст. 1665. URL : https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення – 05.03.2023).

113. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL : http://zakon2.rada.gov.ua/laws/show/2163-19 (дата звернення – 06.03.2023).

114. Про Стратегію кібербезпеки України : Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. Введено в дію Указом Президента України від 15 березня 2016 року № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899. URL : https://zakon.rada.gov.ua/laws/show/n0003525-16#Text (дата звернення – 05.03.2023).

115. Пчеліна О. В. Тактичні завдання розслідування злочинів і криміналістична методика. *Криміналістичний вісник*. 2012. № 2. С. 48–52.

116. Рейнгольд А. В. Концептуальні підходи до побудови

криміналістичної характеристики шахрайства в інтернет-комерції. *Юридична наука*. 2019. № 6. Том 2. С. 73–77.

117. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : дис. … к-та юр. наук : 12.00.09. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 250 с.

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

119. 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.

120. Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : дис. … к-та юр. наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2009. 226 с.

121. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. … к-та юр. наук : 12.00.08 / Університет державної фіскальної служби України. Ірпінь, 2019. 212 с.

122. Розслідування окремих видів злочинів : навч. посібник / за ред. М. А. Погорецького та Д. Б. Сергєєвої. Київ : Алерта, 2015. 536 с.

123. Саінчин О. С. Слідчі ситуації та алгоритми дій в методиці розслідування серійних вбивств. URL : http://www.pravoznavec.com.ua/period/article/22719/%CE (дата звернення – 22.01.2023)

124. Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2005. 588 с.

125. Салтевський М. В., Лукашевич В. Г., Глібко В. М.

Навчально-довідковий посібник з криміналістики. Київ : ВІПОЛ, 1994. 180 с.

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

127. Самойлов С. В. Особливості тактики допиту потерпілих від шахрайств, які пов'язані з купівлею/продажем у мережі Інтернет. *Актуальні питання публічного та приватного права*. 2013. № 3. С. 82–86.

128. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … к-та юр. наук : 12.00.09. Донецький юридичний інститут. Донецьк, 2014. 18 с.

129. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … к-та юр. наук : 12.00.09 / Донецький юридичний інститут. Донецьк, 2014. 226 .

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 : монографія / За науковою редакцією доктора юридичних наук, професора, академіка Академії правових наук України В. І. Борисова. Харків : Право, 2006. 208 с.

132. Синчук В. Л. Кореляційні залежності між елементами криміналістичної характеристики та їх використання у методиці розслідування вбивств : автореф. дис. … канд.. юрид. наук. зі спец. 12.00.09 / Харків, 2004. 20 с.

133. 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.

134. Сисолятін В. В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням

інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

135. Сисолятін В. В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

136. 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.

137. 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. 127–132.

138. Сисолятін В. В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459

139. 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).

140. Сисолятін В. В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням

інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

141. Справа № 161/1919/19. Архів Луцького міськрайонного суду Волинської обл., 2019 р.

142. Справа № 1715/19254. Архів Рівненського міського суду Рівненської обл., 2012 р.

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

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

145. Справа № 303/6112/21. Архів Мукачівського міськрайонного суду Закарпатської обл., 2021 р.

146. Старушкевич А. В. Криміналістична характеристика злочинів : навч. посібник. Київ, 1997. 44 с.

147. Стахівський С. М. Теорія і практика кримінально-процесуального доказування : монографія. Київ, 2005. 272 с.

148. Степанюк Р. Л. Криміналістичне забезпечення розслідування злочинів, вчинених у бюджетній сфері України : монографія / за заг. ред. д-ра юрид. наук, проф. А. Ф. Волобуєва. Харків : НікаНова, 2012. 382 с.

149. 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.

150. Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека*. 2013. № 3 (50). С. 110–115.

151. Степанюк Р. Л. Сутність і практичне значення криміналістичної характеристики злочинів. *Порівняльно-аналітичне право.* 2014. № 5. С. 398–400.

152. Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність : системний підхід. *Інформаційні технології і засоби навчання.* 2015. Т. 49. № 5. С. 41–49.

153. Тертишник В. М. Науково-практичний коментар до Кримінально-процесуального кодексу України / Київ : Видавництво А.С.К., 2003. 1056 с.

154. Тіщенко В. В. Криміналістичні технології в теорії і практиці розслідування. *Актуальні проблеми держави і права* : зб. наук. праць. 2008. Вип. 44. С. 18–24.

155. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

156. Тіщенко В. В. Щодо використання спеціальних знань у кримінальному провадженні. Матеріали Всеукраїнської науково-практичної Інтернет-конференції (27 листопада 2013 року, м. Одеса). Одеса : «Юридична література», 2013. С. 349–353.

157. Томін С. В. Об’єкт та предмет профілактики кримінальних правопорушень як окремого вчення криміналістики. *Прикарпатський юридичний вісник*. Випуск 3(12), 2016. С. 123-127.

158. Узунова О. В., Калюга К. В. Проблеми прийомів аналізу отриманої з місця події інформації та обґрунтування припущень стосовно особи злочинця. URL : http://bo0k.net/index.php?bid=18860&chapter=1&p=achapter (дата звернення – 12.02.2023)

159. Хижняк Є. С. Типові слідчі ситуації при розслідуванні статевих злочинів. *Південноукраїнський правничий часопис*. 2012. № 4. С. 197–199.

160. Чаплинська Ю. А. Особа злочинця як елемент криміналістичної характеристики злочинів. *Актуальні проблеми юриспруденції*. 2019. № 6. С. 181–184.

161. Чаплинський К. О. Тактика пред’явлення для впізнання : навчально-методичний посібник. Дніпропетровськ : Дніпропетровський

державний університет внутрішніх справ, 2007. 103 с.

162. Чаплинський К. О. Тактика проведення окремих слідчих дій : монографія. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ, 2006. 308 с.

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

164. Чернявський С. С., Довбаш Р. С. Протидія злочинам, пов'язаним з незаконним відшкодуванням ПДВ : наук.-практ. посіб. Київ : Хай-Тек Прес, 2009. 216 с.

165. 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.

166. 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.

167. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 2. С. 58–68.

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

169. 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, 8 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. С. 220-222.

170. Чорноус Ю. М. Криміналістичне забезпечення як наукова категорія та практичне завдання криміналістики. *Проблеми правознавства та*

правоохоронної діяльності. 2012. № 1. С. 149–155.

171. 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.

172. 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.

173. Шалгунова С. А. Особа злочинця за уявленнями дореволюційних вітчизняних юристів: антропологічна та соціологічна школи. *Право і суспільство*. 2011. № 6. С. 157–164.

174. Шевчук В. М. Слідча ситуація: повнота, структура, види та її значення для оптимізації розслідування злочинів. *Юридичний науковий електронний журнал*. № 1. 2014. С. 142–150.

175. Шепітько В. Ю. Криміналістична тактика (системно-структурний аналіз) : монографія. Харків : Харків юридичний, 2007. 432 с.

176. Шепітько В. Ю. Особа потерпілого в системі криміналістичної характеристики злочинів. *Проблеми законності* : республік. міжвід. наук. зб. / відп. ред. В. Я. Тацій. Харків : Нац. юрид. акад. України, 2008. Вип. 93. С. 168–174.

177. Шеремет А. П. Криміналістика : навч. посіб. для студ. вищ. навч. закл. 2-ге вид. Київ : Центр учбової літ., 2009. 472 с.

178. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : автореф. дис. … докт. юрид. наук : спец. 12.00.09 / Національний юридичний університет ім. Ярослава Мудрого. Харків : 2011. 32 с.

179. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : монографія. Харків : Харків юридичний, 2010.

320 с.

180. Юридична психологія : підручник / за заг. ред. Л. І. Казміренко, Є. М. Моісеєва. Київ : КНТ, 2007. 360 с.

181. Clay, W. Computer Attack and Cyberterrorism : Vulnerabilities and Policy Issues for Congress. URL : https://digital.library.unt.edu/ark:/67531/metacrs6315/m1/1/ (дата звернення – 06.02.2023).

182. Dorothy, E. Denning Activism, Hacktivism, and Cyberterrorism : The Internet as a Tool for Influencing Foreign Policy. URL : https://www.semanticscholar.org/paper/Activism%2C-Hacktivism%2C-and-Cyberterrorism%3A-the-As-a-Denning/829b21633c51252429abcb1ac717ecc4efc64566 (дата звернення – 27.03.2023).

183. James, A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. URL : https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats (дата звернення – 16.03.2023).

184. Louise, I. Shelley Organized Crime, Terrorism and Cybercrime. URL : https://www.ojp.gov/ncjrs/virtual-library/abstracts/organized-crime-terrorism-and-cybercrime (дата звернення – 06.02.2023).

185. Phil, Williams Organized Crime and Cybercrime : Synergies, Trends, and Responses. URL : https://www.crime-research.org/library/Cybercrime.htm (дата звернення – 21.04.2023).

186. Reznik, O., Fomenko, A., Melnychenko, A., Pavlova, N., Prozorov, A. Features of the initial stage of investigating fraud with financial resources in cyberspace. *Amazonia Investiga.* 2021. Volumer10. Issue 41: pp. 141–150.

187. Sysoliatin, V. Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

188. Sysoliatin, V. The further stage of the investigation of criminal offences involving internet banking (issues of concern). *Entrepreneurship,*

Economy and Law. 2023. № 6. pp. 89–94.

189. Yefimov M., Omarov Y. Scientific debates on the preventive activities of authorized persons as part of the methodology for investigating criminal offences against morality. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs* : Scientific Journal. 2021. Special Issue № 1 (114). pp. 114–119.

190. Yefimov M., Pavlova N., Fedchenko V., Pletenets V., Kryvopusk O. Experiencia extranjera en regulación jurídica de investigación de fraudes. *Revista De La Universidad Del Zulia*. *13*(38). 2022. pp. 159-168.

191. Zarubei, V., Humin, O., Rymarchuk, O. Concerning the need for improvement of the methodology of investigating frauds and development of methods of investigation of this individual types. *Baltic Journal of Economic Studies,* 2018. Volume 4. Number 5. pp. 63–66.

ДОДАТКИ

Додаток А

Результати вивчення

247 кримінальних проваджень за напрямом дослідження (Волинська, Дніпропетровська, Донецька, Закарпатська, Запорізька, Івано-Франківська, Київська, Кіровоградська, Львівська, Миколаївська, Одеська, Сумська, Ужгородська, Харківська та Чернівецька області, м. Київ)

№	Досліджувані питання	%
	КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА	
1	**Обстановка вчинення кримінального правопорушення**	
	1.1. Місце вчинення протиправних дій	
	1) місця розташування електронно-обчислювальної техніки, з якої вчинялись протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон)	**61**
	2) місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери	**21**
	3) місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу	**12**
	4) інші	**6**
2	**Способи вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу**	
	2.1. Повноструктурний	**99**
	2.2. Підготовка до вчинення	**100**
	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	
	2.3. Способи безпосереднього вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу	**100**
	1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг)	
	2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	
	3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення	
	4) розповсюдження шкідливих програмних чи технічних засобів або їх збут з використанням мережі Інтернет	
	5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах	
	6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів	
	2.4. Способи приховування	**99**
	1) знищення обладнання, що використовувалось для вчинення протиправних дій	

	2) приховування створеного шкідливого програмного забезпечення за допомогою легального програмного забезпечення	
	3) використання перетворення ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються протиправні дії	
	4) дача неправдивих показів при проведенні окремих процесуальних дій (в тому числі – неправдиве алібі)	
	5) відмова від дачі показань	
3	**Відомості про слідову картину протиправного діяння**	
	3.1 Матеріальні слід	**37**
	3.2. Електронні сліди (віртуальні, цифрові, комп'ютерні)	**100**
	3.3. Ідеальні сліди	**39**
5	**Особа потерпілого**	
	5.1. Віктимогенні групи потерпілих:	
	1) працівники фінансових установ, підприємств та організацій різних форм власності	
	2) клієнти фінансових установ, підприємств та організацій різних форм власності	
	3) родичі клієнтів фінансових установ, підприємств та організацій різних форм власності	
6	**Дані про особу злочинця**	
	6.1. Стать:	
	1) чоловіча	**91**
	2) жіноча	**9**
	6.2. Вік:	
	1) від 16 до 20 років	**8**
	2) від 20 до 30 років	**42**
	3) від 30 до 40	**26**

	4) від 40 до 50	**19**
	5) особи віком 50 років і старше	**5**
	6.3. Освіта:	
	1) базова середня	**1**
	2) середня	**2**
	3) середня спеціальна	**4**
	4) базова вища	**15**
	5) вища	**79**
	6.4. Сімейний стан:	
	1) у шлюбі	**24**
	2) ні	**76**
	6.5. Рід занять:	
	1) учень (студент)	**9**
	2) працюючий	**91**
	3) у сфері фінансової діяльності та сфері комп'ютерних технологій	**81**
	6.6. Наявність судимості:	**4**
	6.7. Протиправні діяння вчинено у стані сп'яніння:	
	1) алкогольного	**1**
	2) наркотичного	**1**
	6.8. Особи, які вчиняють кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, відрізняються досить високим інтелектуальним рівнем:	
	1) так	**85**
	2) ні	**15**

	ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ	
7	**Первинна інформація, яка була підставою для внесення відомостей до Єдиного реєстру досудових розслідувань за фактом учинення кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, потрапляли до підрозділів правоохоронних органів наступним чином:**	
	1) заяви, листи та повідомлення від громадян, які є потерпілими від досліджуваних протиправних діянь	**77**
	2) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене протиправне діяння або стали його свідками	**9**
	3) повідомлення працівників установ, підприємств та організацій	**3**
	4) матеріали досудового розслідування, виділені з інших кримінальних проваджень	**6**
	5) матеріали, отримані під час проведення НСРД та розшукових заходів	**5**
8	**Типові слідчі ситуації початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу:**	
	1) скоєно кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, має місце достатня доказова база, особу правопорушника встановлено	**6**
	2) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника не встановлено	**64**
	3) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника встановлено, та протиправні дії приховані під легальну фінансову діяльність	**9**
	4) скоєно протиправне діяння, має місце заява потерпілого,	**21**

	відсутня будь-яка доказова база	
	СЛІДЧІ (РОЗШУКОВІ) ДІЇ, НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ТА ІНШІ ПРОЦЕСУАЛЬНІ ДІЇ:	
9	**Які СРД та процесуальні дії проводились:**	
	1) огляд місця події	**98**
	2) допит потерпілого або представника потерпілої сторони	**100**
	3) огляд електронної інформації	**94**
	4) допит свідка	**100**
	5) тимчасовий доступ до речей і документів	**79**
	6) допит підозрюваного	**100**
	7) обшук	**91**
	8) призначення та проведення експертиз	**100**
	9) слідчий експеримент	**1**
	10) пред'явлення особи для впізнання	**4**
	а) за голосом	**3**
	б) в натурі	**1**
	11) одночасний допит раніше допитаних осіб	**82**
	12) огляд документів	**53**
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. Об'єкти, які вилучались:	
	1) електронно-обчислювальна техніка, за допомогою якої здійснювалось втручання в роботу інтернет-мереж для їх дестабілізації або отримання відомостей, необхідних для	

	реалізації операцій в інтернет-банкінгу (комп'ютери, планшети, ноутбуки, смартфони)	
	2) реквізити карток, що викрадені з серверів магазинів електронної торгівлі, платіжних і розрахункових систем, з персональних ґаджетів користувачів	
	3) фотографії, відеозаписи, на яких наявні дані, що мають значення для кримінального провадження	
	4) квитанції про здійснення банківських операцій	
	5) смартфони або інші ґаджети, в яких наявна адресна книга (ПІБ й адреси клієнтів фінансових установ, підприємств та організацій різних форм власності)	
	6) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб	
12	**Які НСРД проводились найчастіше:**	
	1) спостереження за об'єктом	
	2) прослуховування телефонних переговорів	
13	**Допит:**	
	13.1. Ситуації за конфліктністю:	
	1) безконфліктні	**19**
	1) конфліктні	**81**
14	**Одночасний допит:**	**82**
	14.1. Між ким проводився:	
	1) між підозрюваним та потерпілим	**91**
	2) між підозрюваним та свідками	**2**
	3) між підозрюваними особами	**7**
	14.2. Результат одночасного допиту:	
	1) підозрюваний повністю або частково засвідчив свідчення, які раніше заперечував	**63**
	2) підозрюваний знову заперечував свідчення	**37**

15	**Залучення спеціаліста до СРД, НСРД та інших процесуальних дій:**	
	1) огляд місця події	**100**
	2) огляд електронної інформації	**100**
	3) обшук	**98**
	4) тимчасовий доступ до речей та документів	**51**
	5) допит	**41**
	6) зняття інформації з транспортних телекомунікаційних мереж та електронних систем	**100**
16	**Експертизи:**	
	16.1. Об'єкти, що направляються на експертизу:	
	1) власні ґаджети потерпілого (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори)	
	2) власні ґаджети підозрюваного (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори)	
	3) флеш-накопичувачі	
	4) жорсткі диски	

Додаток Б

Зведені результати опитувань

151 працівника прокуратури, 316 слідчих, 376 працівників оперативних підрозділів та 84 працівників експертних установ МВС України

	З а п и т а н н я	**%**
1.	**Вкажіть Ваш вік:**	
	До 25 років	**41**
	25-30 років	**28**
	31-40 років	**24**
	41 рік і старше	**7**
2.	**Вкажіть стаж практичної роботи:**	
	до 1 року	**8**
	від 1 до 3 років	**21**
	від 3 до 5 років	**34**
	від 5 до 10 років	**25**
	більше 10 років	**12**
3.	**Чи розслідували Ви або брали участь у розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу:**	
	так	**100**
	ні	**0**
4.	**Чи мали місце у Вашому підрозділі випадки розслідування кримінальних правопорушень, пов'язаних із використанням 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 кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу:**	
	так	**61**
	ні	**39**
6.	**Чи вважаєте Ви, що розслідування кримінальних правопорушень даної категорії потребує відповідної кваліфікації уповноваженої особи у цьому напряму:**	
	так	**98**
	ні	**2**
7.	**Чи згодні Ви з твердженням, про необхідність розроблення криміналістичної характеристики правопорушень, пов'язаних із використанням інтернет-банкінгу, в розрізі докладної побуди кореляційних зв'язків між окремими її елементами:**	
	так	**97**
	ні	**3**
8.	**На Вашу думку, якими чинниками зумовлена низька якість розслідування кримінальних проваджень досліджуваної категорії та незначна кількість викритих й притягнутих до відповідальності злочинців:**	
	відсутність чіткої взаємодії й належної координації окремих підрозділів Національної поліції (зокрема, співробітників кіберполіції та слідчих)	**71**
	невчасне здійснення СРД, НСРД та інших процесуальних заходів	**61**
	поверхневе використання техніко-криміналістичних засобів під час проведення окремих процесуальних дій та ігнорування залучення відповідних спеціалістів	**79**
	відсутність міжнародної практики розслідування кримінальних	**82**

	правопорушень, пов’язаних із використанням інтернет-банкінгу	
	порушення послідовності дій під час збирання доказів на початковому етапі кримінального провадження	**91**
9.	**Які заходи можуть застосовуватися для приховування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу:**	
	знищення обладнання, що використовувалось для вчинення протиправних дій	**41**
	приховування створеного шкідливого програмного забезпечення за допомогою легального програмного забезпечення	**44**
	використання перетворення ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються протиправні дії	**78**
	дача неправдивих показів при проведенні окремих процесуальних дій (в тому числі – неправдиве алібі)	**31**
	відмова від дачі показань	**65**
10.	**Чи виникають під час допиту підозрюваного в досліджуваній категорії кримінальних проваджень конфліктні ситуації:**	
	так	**81**
	ні	**19**
11.	**Назвіть, будь ласка, ситуації, які виникали під час проведення допиту підозрюваного при розслідуванні кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу:**	
	підозрюваний повідомляє інформацію про обставини протиправного, однак не висвітлює її у повному обсязі	**26**
	– це відбувається через страх помсти зі сторони співучасників	**45**
	– через залежність від його організатора	**21**
	– заінтересованістю в результатах провадження	**34**
	підозрюваний не бажає давати повні та щирі показання – факт конфліктної ситуації	**29**
	підозрюваний цілком відмовляється від комунікації з уповноваженою особою, відмовляється давати показання, а також	**21**

	брати участь у проведенні окремих СРД	
	підозрюваний не заперечує факт і зміст протиправного діяння, однак спростовує свою участь у його вчиненні	**5**
12.	**Які, на Вашу думку, найбільш доцільні тактичні прийоми під час проведення допиту підозрюваного при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу:**	
	створення уявлення про інформованість уповноваженої особи	**89**
	швидкий темп допиту	**56**
	використання фактора раптовості	**57**
	створення напруги	**69**
	пред'явлення речових доказів	**33**
	застосування відеозапису	**45**
13.	**Назвіть, будь ласка, головні форми використання спеціальних знань під час розслідування досліджуваної категорії протиправних діянь:**	
	консультативно-довідкова допомога	**34**
	участь спеціаліста у проведенні СРД, НСРД	**81**
	призначення експертиз	**100**
	інше	**19**
14.	**На Вашу думку, які фактори позначаються на поширенні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу?**	
	недосконалість законодавства у сфері інформаційних відносин	**72**
	недосконалість державного контролю за сферою використання інтернет-банкінгу	**48**
	брак ефективної взаємодії правоохоронних органів між собою	**41**
	віктимна поведінка (недбалість, необізнаність, зайва довірливість тощо) потерпілих	**95**

	інше	**31**

Додаток В

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

2. 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).

3. 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. 127–132.

4. Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

5. 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.

6. 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.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37. (публікація тез)

8. Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24. (публікація тез)

9. Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23. (публікація тез)

10. 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. (публікація тез)

Додаток Г

Акти впровадження результатів дисертаційного дослідження

ЗАТВЕРДЖУЮ
Проректор
Національної академії
внутрішніх справ
доктор юридичних наук, професор
заслужений діяч науки і техніки України
полковник поліції
Сергій ЧЕРНЯВСЬКИЙ
2023 року

АКТ
впровадження у науково-дослідну діяльність та освітній процес Національної академії внутрішніх справ результатів дисертаційного дослідження

Про впровадження у науково-дослідну діяльність та освітній процес Національної академії внутрішніх справ основних результатів дисертаційного дослідження Сисолятіна Валерія Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням 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:

голови: заступника начальника навчально-методичного відділу Національної академії внутрішніх справ, кандидата юридичних наук, капітана поліції Бистрицького Б.Ю.

членів комісії: професора кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктора юридичних наук, професора, підполковника поліції Чорноус Ю.М.

професора кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидата юридичних наук, професора, полковника поліції Пясковського В.В.

відповідно до Пріоритетних напрямів наукових досліджень Національної академії внутрішніх справ на 2022-2023 навчальний рік склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Сисолятіна Валерія Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних

із використанням 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 Національної академії внутрішніх справ для подальшої розробки проблемних питань методики розслідування злочинів у сфері економіки. Результати дисертації відображено у наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (статтях і тезах доповідей на конференціях):

Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

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).

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. 127–132.

Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

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.

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.

Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матер. Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей В.В. Сисолятіна, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також будуть враховані профільними кафедрами Національної академії внутрішніх справ при проведенні наукових досліджень.

Заступник начальника навчально-методичного відділу
Національної академії внутрішніх справ
кандидат юридичних наук,
капітан поліції **Богдан БИСТРИЦЬКИЙ**

Професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ
доктор юридичних наук, професор
підполковник поліції **Юлія ЧОРНОУС**

Професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ
кандидат юридичних наук, професор
полковник поліції **Вадим ПЯСКОВСЬКИЙ**

ЗАТВЕРДЖУЮ
Декан факультету № 1
Харківського національного
університету внутрішніх справ
кандидат юридичних наук, доцент
підполковник поліції

Віталій РОМАНЮК

«06» 04.2003 2023 року

АКТ
впровадження у науково-дослідну діяльність та освітній процес Харківського національного університету внутрішніх справ результатів дисертаційного дослідження Сисолятіна В.В. «Розслідування кримінальних правопорушень, пов'язаних із використанням 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:

голови: завідувача кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, кандидата юридичних наук, доцента Корнієнка В.В.

членів комісії: професора кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктора юридичних наук, професора Степанюка Р.Л.

професора кафедри кримінального процесу та організації досудового слідства факультету № 1 Харківського національного університету внутрішніх справ, кандидата юридичних наук, доцента Глобенка Г.І.

склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Сисолятіна Валерія Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням 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 дисертаційного дослідження Сисолятіна Валерія

Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» використовуються в освітньому процесі та науково-дослідницькій роботі Харківського національного університету внутрішніх справ з метою подальшої розробки проблемних питань протидії економічній злочинності, насамперед, у сфері інтернет-комерції, а також методики розслідування окремих видів кримінальних правопорушень.

Основні результати дисертації відображено у наступних наукових публікаціях здобувача, зокрема:

Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

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).

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. 127–132.

Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

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.

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.

Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

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

Члени комісії дійшли висновку, що надані матеріали свідчать про відповідність спеціальності 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність; належний науковий, теоретичний та практичний рівень розробки дисертаційного дослідження на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу»; актуальність, вчасність і практичну значущість дослідження, грунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення

кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України. Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Харківського національного університету внутрішніх справ при проведенні наукових досліджень.

Голова комісії:
завідувач кафедри криміналістики,
судової експертології та домедичної підготовки
Харківського національного
університету внутрішніх справ
кандидат юридичних наук, доцент **Василь КОРНІЄНКО**

Члени комісії:
професор криміналістики,
судової експертології та домедичної підготовки
Харківського національного
університету внутрішніх справ
доктор юридичних наук, професор **Руслан СТЕПАНЮК**

професор кафедри кримінального
процесу та організації досудового слідства
Харківського національного
університету внутрішніх справ
кандидат юридичних наук, доцент **Геннадій ГЛОБЕНКО**

ПІДПИС ЗАСВІДЧУЮ
Факультет №1 ХНУВС
«06» 04 2023

ЗАТВЕРДЖУЮ
Директор
Навчально-наукового інституту права
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
доктор юридичних наук, професор
заслужений юрист України

Анатолій КИСЛИЙ

«25» 05 2023 року

АКТ
впровадження в освітній процес і наукову діяльність Навчально-наукового інституту права ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» результатів дисертаційного дослідження

Про впровадження в освітній процес і наукову діяльність ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» дисертаційного дослідження Сисолятіна Валерія Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням 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:

голови: завідувача кафедри правоохоронної та антикорупційної діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доктора юридичних наук, професора Заросила В.О.

членів комісії: заступника директора Навчально-наукового інституту права ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», кандидата юридичних наук, доцента Тимошенка Ю.П.

професора кафедри правоохоронної та антикорупційної діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доктора юридичних наук, доцента Козаченка О.І.

відповідно до Положення про організацію освітнього процесу і наукової діяльності в ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія

управління персоналом» склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Сисолятіна Валерія Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням 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:

Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал.* 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

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).

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. 127–132.

Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law.* 2023. № 5. pp. 112–117.

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.

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.

Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

Члени комісії дійшли висновку, що надані здобувачем Науково-дослідного інституту публічного права В.В. Сисолятіним матеріали (наукові статті та тези доповідей) свідчать про належний науковий, методологічний та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, відображені у науково-методичних матеріалах навчальних дисциплін з кримінального права, кримінального процесу та криміналістики для здобувачів вищої освіти бакалавра і магістра.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та можуть використовуватися в освітньому процесі та науковій діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» при підготовці здобувачів вищої освіти.

Голова комісії: **Володимир ЗАРОСИЛО**

Члени комісії: **Юрій ТИМОШЕНКО**

Олександр КОЗАЧЕНКО

ЗАТВЕРДЖУЮ
Директор
Дніпропетровського НДЕКЦ МВС
кандидат юридичних наук, доцент

Володимир КОРОТАЄВ

_____ 2023 р.

АКТ
впровадження результатів дисертаційного дослідження
у практичну діяльність Дніпропетровського НДЕКЦ МВС

Про впровадження у практичну діяльність Дніпропетровського НДЕКЦ МВС результатів дисертаційного дослідження Сисолятіна В.В. на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням 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: т.в.о. заступника завідувача лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС Геннадія Комизи

Членів комісії: завідувача сектору дактилоскопічного обліку лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС Ольги Гейко

головного судового експерта лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС Олени Олександрової

Комісія відповідно до Положення про організацію проведення науково-дослідних та дослідно-конструкторських робіт у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15 травня 2007 року № 154 склала

цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Сисолятіна Валерія Вікторовича на тему: «Розслідування кримінальних правопорушень, пов'язаних із використанням 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 фахових наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

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).

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. 127–132.

Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

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.

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.

Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Виклики сучасності та наукові підходи до їх вирішення : матер. Міжнародної науково-практичної конференції* (м. Київ, 12-13 серпня 2020 р). Київ : Науково-дослідний інститут публічного права, 2020. С. 35–37.

Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення : матер. Міжнародної науково-практичної конференції* (м. Київ, 22-23 вересня 2021 р.). Київ : Науково-дослідний інститут публічного права, 2021. С. 22–24.

Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матер. Міжнарод. наук.-практ. конференції* (м. Київ, 14–15 черв. 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

Комісія вважає, що представлені матеріали дисертаційного дослідження, фахові наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також можуть бути впроваджені у діяльність Дніпропетровського НДЕКЦ МВС України.

Голова комісії: **Геннадій КОМИЗА**

Члени комісії: **Ольга ГЕЙКО**

Олена ОЛЕКСАНДРОВА