НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

УДК 343.98: 343.131

МАЛЮТІН ЕДУАРД ВІКТОРОВИЧ

ДИСЕРТАЦІЯ

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ Е-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

Е. В. Малютін

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

Київ – 2024

АНОТАЦІЯ

Малютін Е. В. Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-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; Дніпровський державний університет внутрішніх справ, Київ, 2024.

У дисертаційній роботі на монографічному рівні опрацьовано теоретичні та праксеологічні засади методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. Запропоновано систему окремої методики розслідування, в яку включено складові з огляду на організаційно-тактичні особливості здійснення кримінальних проваджень, розпочатих за фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, зокрема, додано такі, як: криміналістична характеристика кримінальних правопорушень; розгляд первинної інформації, а також особливості занесення відповідних даних в Єдиний реєстр досудових розслідувань; обставини, котрі варто з'ясовувати під час розслідування; типові слідчі ситуації розслідування; початковий етап розслідування (проведення слідчих (розшукових) дій, НСРД та розшукових заходів); подальший етап розслідування (проведення слідчих (розшукових) дій, НСРД та інших процесуальних заходів); використання спеціальних знань у кримінальному провадженні; тактичні операції; взаємодія підрозділів правоохоронних органів; встановлення причин та умов, що сприяли вчиненню протиправного діяння.

Вироблено структуру криміналістичної характеристики досліджуваних протиправних діянь, в якій виокремлено такі елементи: спосіб та обстановку кримінального правопорушення, слідову картину, особу злочинця, особу

потерпілого.

Удосконалено теоретичні концепції класифікації типових способів підготовки, безпосереднього вчинення та приховування протиправних діянь, учинених із використанням е-банкінгу.

Сформовано систему відомостей стосовно обстановки вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, крізь призму просторових, часових та соціальних чинників. До обстановки віднесено такі складові: 1) час, протягом якого здійснювалися злочинні дії; 2) час, коли настали наслідки від протиправних дій; 3) місце реалізації злочинних дій (віртуальне середовище, в якому вчиняються дії, і місця, де знаходяться точки доступу – IP-адреси).

Надано характеристику слідової картини кримінальних правопорушень шляхом надання відомостей стосовно матеріальної (ЕОТ, папілярні візерунки), особистісної (показання потерпілих, свідків, підозрюваних) та віртуальної (пам'ять ЕОТ, кеш-пам'ять серверів інтернет-провайдерів, пам'ять смартфонів, кеш-пам'ять електронного реєстру термінала чи банкомата) інформації.

Сформовано ймовірний «портрет» особи злочинця. З'ясовано, що особам, які вчиняють кримінальні правопорушення, пов'язані з використанням е-банкінгу, притаманні високий рівень інтелекту, винахідливість та комунікабельність. Властивою характеристикою особи злочинця (хакери, фішери, фрікери, спамери, кіберсквотери, спеціалісти з програмного забезпечення та використання ЕОТ) є особливий вид ознак – інтелектуальні. Ці особи володіють спеціальними знаннями й навичками у сфері електронного бізнесу, е-комерції, інтернет-торгівлі, здійснення банківських операцій, використання цифрових технологій, комп'ютерного програмування та ін. Здебільшого це чоловіки віком 20–40 років, які мають базову або повну вищу освіту.

Виокремлено віктимогенні групи потерпілих, зокрема: а) фізичні особи, які здійснювали купівлю-продаж товарів і послуг на онлайн-

платформах та інтернет-аукціонах із використанням е-банкінгу; б) працівники фінансових установ, підприємств та організацій різних форм власності; в) їхні клієнти; г) родичі клієнтів; д) юридичні особи – при здійсненні матеріально-технічного постачання та інших заходів у випадках використання інтернет-банкінгу.

Конкретизовано особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. Встановлено, що початкові відомості, котрі надійшли до правоохоронних органів і стали приводом для внесення інформації до ЄРДР за фактом учинення досліджуваного виду кримінальних правопорушень.

Вирізнено типові слідчі ситуації, що формуються на початковому етапі розслідування кримінальних правопорушень: 1) вчинено кримінальне правопорушення, пов'язане з використанням е-банкінгу, наявна достатня кількість доказової інформації, встановлено особу злочинця; 2) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, особу злочинця не встановлено; 3) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, встановлено особу злочинця, але злочинні дії замасковані під легальну фінансову діяльність; 4) вчинено кримінальне правопорушення, наявна заява потерпілої особи, відсутня будь-яка доказова інформація.

Окреслено систему тактичних завдань, що мають місце у діяльності працівників правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також комплекс заходів для їх вирішення в межах проведення низки тактичних операцій.

Запропоновано перелік питань, котрі необхідно з'ясовувати під час допиту підозрюваного, як-от: у який спосіб було вчинено протиправні дії (безконтактно – за допомогою мережі Wi-Fi загального користування, домашньої мережі Wi-Fi, контактно – за допомогою заволодіння ЕОТ зі встановленими паролями); які способи використовувалися для входження у застосунок для е-банкінгу (застосування спам-ботів; застосування реквізитів

картки, отриманої у користувача або з сайтів фіктивних онлайн-магазинів; застосування вірусних програм); протягом якого терміну були скоєні кримінальні правопорушення та які супутні протиправні діяння було вчинено; чи були вчинені протиправні дії ОГ чи ЗО; якщо так, то які функції кожного з їх учасників та яка система розподілу грошових коштів між ними; які засоби застосовувалися під час вчинення протиправних дій (технічні – ЕОТ, модеми, смартфони, маршрутизатори; програмні – web-браузери, VPN); якою була загальна сума грошових коштів (валюта, криптовалюта) на момент закінчення вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Визначено організаційно-тактичні особливості взаємодії підрозділів Національної поліції України (кіберполіції, слідства), а також форми взаємодії, зокрема: здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, НСРД та інших заходів, обмін інформацією, надання уповноваженій особі відомостей, що зібрані у процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення інформації до ЄРДР, спільне планування розшукових заходів, здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, котрі мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними матеріалами.

Сформовано перелік профілактичних заходів, що можуть проводитись уповноваженими особами правоохоронних органів (слідства, дізнання, кіберполіції) стосовно усунення причин і умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а саме: повідомлення громадян за допомогою засобів масової інформації про юридичну відповідальність (адміністративну, цивільну, кримінальну) за протиправні дії; реалізація профілактичного впливу на громадян шляхом використання окремих процесуальних дій із метою здійснення профілактики; встановлення осіб, схильних до антисуспільної поведінки у сфері

використання електронно-обчислювальної техніки, а також їх подальше занесення до обліку в підрозділах кіберполіції; участь працівників кіберполіції у тематичних передачах, круглих столах або ток-шоу; вивчення матеріалів кримінальних проваджень для з'ясування та усунення умов і причин, що сприяли вчиненню протиправних діянь; організація дискусій у ЗМІ (електронних та друкованих), в яких обговорюються кіберзлочинність та її вплив на суспільство; інформування громадян у соціальних мережах, ЗМІ, месенджерах щодо фактів учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (фішингу, кардингу, спамінгу).

Встановлено, що однією з головних причин неефективності заходів із запобігання кримінальним правопорушенням, що пов'язані з використанням е-банкінгу, залишається низький рівень обізнаності слідчих та працівників оперативних підрозділів Національної поліції України щодо типових злочинних схем під час здійснення незаконних банківських операцій та напрямів збирання електронних доказів, встановлення правопорушників за цифровою слідовою картиною, особливостей документування злочинних дій у кіберпросторі та ін.

Запропоновано пропозиції стосовно внесення норми в чинний КПК України, в якій буде вказано обов'язок працівників правоохоронних органів (слідчих, дізнавачів, детективів, прокурорів) забезпечувати усунення причин та умов, що сприяли вчиненню протиправних діянь.

Розкрито тактичні операції щодо збирання первинних даних про обставини злочинної події та виявлення ознак досліджуваних протиправних діянь, а саме серед них визначено такі, як: «Встановлення характеру події кримінального правопорушення», «З'ясування місця та часу вчинення протиправного діяння», «Встановлення способу вчинення протиправного діяння (фішинг, застосування шпигунських програм, спам-ботів)», «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», «З'ясування особи потерпілого та її віктимної поведінки, а також перевірка їхніх зв'язків» та ін.

На основі узагальнення судово-слідчої практики запропоновано перелік слідчих (розшукових) дій, НСРД та інших процесуальних заходів, необхідних для ефективного здійснення тактичних операцій у кримінальному провадженні. Виявлено тактичні помилки, що їх припускаються уповноважені особи під час реалізації таких операцій.

Розроблено систему заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», зокрема: допити потерпілих; встановлення та допити свідків; огляд електронно-обчислювальної техніки; зняття інформації з електронних інформаційних систем або її частини; встановлення місцезнаходження радіоелектронного засобу; встановлення особи злочинця та оголошення її у розшук; встановлення місцезнаходження злочинця; затримання злочинця; направлення вимог щодо надання правоохоронними органами, органами державної влади та органами місцевого самоврядування інформації, котра має значення для кримінального провадження за фактами вчинення протиправних діянь, пов’язаних із використанням е-банкінгу; обшуки за місцем проживання та в інших місцях перебування злочинця; допит підозрюваного для встановлення ймовірних співучасників кримінального правопорушення; проведення затримання співучасників (членів ОЗГ, які задіяні до злочинної діяльності); обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерполу, Європолу) стосовно реагування на кіберзлочини; призначення та проведення судових експертиз.

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

– *законотворчій діяльності* – для удосконалення законодавства у сфері попередження кримінальних правопорушень, пов’язаних із використанням е-банкінгу, викладено низку рекомендацій стосовно внесення змін і доповнень до діючого Кримінального процесуального кодексу

України;

– *науковій діяльності* – для удосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Національної академії внутрішніх справ від 26.02.2024, Харківського національного університету внутрішніх справ від 29.02.2024, Дніпропетровського державного університету внутрішніх справ від 11.03.2024);

– *освітньому процесі* – при викладанні навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Оперативно-розшукова діяльність», «Криміналістичні засоби та методи розслідування кримінальних правопорушень». а також при підготовці підручників і навчальних посібників (акти впровадження Національної академії внутрішніх справ від 27.02.2024, Інституту права та суспільних відносин Відкритого міжнародного Університету розвитку людини «Україна» від 13.03.2024);

– *правозастосовній діяльності* – для вдосконалення діяльності органів досудового розслідування, оперативних та експертних підрозділів Національної поліції України (акти впровадження Управління стратегічних розслідувань в Дніпропетровській області ДСР Національної поліції України від 21.09.2023).

Ключові слова: е-банкінг, банківські операції, е-бізнес, електронний переказ, транзакція, кіберзлочини, комерція, інтернет-банкінг, досудове розслідування, методика, криміналістична характеристика, кримінальне правопорушення, слідчі (розшукові) дії, експертиза, спеціальні знання.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано
основні наукові результати дисертації:

1. Малютін Е. В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Т. 2. С. 143–147.

2. Малютін Е. В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Т. 2. С. 122–128.

3. Малютін Е. В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 425–428. URL : http://www.lsej.org.ua/9_2021/9_2021.pdf.

4. Малютін Е. В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія : Право.* 2022. № 2. С. 232–236.

5. Малютін Е. В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

6. Малютін Е.В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 77–82.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Малютін Е. В. Обстановка вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

8. Малютін Е. В. Особливості початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням е-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. 171–173.

9. Малютін Е. В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 139–141.

10. Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146.

SUMMARY

Maliutin E. V. Basics of the methodology of investigation of criminal offenses related to the use of e-banking. – *Qualifying scientific work on manuscript rights.*

The thesis is for candidate degree of legal sciences (doctor of philosophy) in the field 12.00.09 – Criminal Procedure and Forensic Sciences; Judicial Examination; Operational-Search Activity (081 – Law). – Research Institute of Public Law; Dnipro State University of Internal Affairs, Dnipro, 2024.

The theoretical and praxeological foundations of the methodology of investigation of criminal offenses related to the use of e-banking are elaborated in the dissertation at the monographic level. A system of a separate investigation methodology is proposed, which includes components taking into account the organizational and tactical features of criminal proceedings initiated upon the commission of criminal offenses related to the use of e-banking, in particular, the following are added: forensic characteristics of criminal offenses; consideration of primary information, as well as features of entering relevant data into the Unified Register of Pretrial Investigations; circumstances that should be clarified during the investigation; typical investigative situations of the investigation; the initial stage of the investigation (conduct of investigative (search) actions, secret investigative (search) actions and search measures); the further stage of the investigation (conduct of investigative (search) actions, secret investigative (search) actions and other procedural measures); use of special knowledge in criminal proceedings; tactical operations; interaction of law enforcement units; establishing the reasons and conditions that contributed to the commission of an illegal act.

The structure of the criminalistic characteristics of the investigated illegal acts has been developed, in which such elements as: the method and situation of the criminal offense, the trace picture, the identity of the criminal, the identity of

the victim are distinguished.

The theoretical concepts of classification of typical methods of preparation, direct commission and concealment of illegal acts committed using e-banking have been improved.

A system of information regarding the circumstances of the commission of criminal offenses related to the use of e-banking was formed through the prism of spatial, temporal and social factors. The situation includes the following components: 1) the time during which criminal actions were carried out; 2) the time when the consequences of illegal actions occurred; 3) place of implementation of criminal actions (virtual environment in which actions are committed and places where access points are located – IP addresses).

The characterization of the trace picture of criminal offenses is provided by providing information about the material (ECT, papillary patterns), personal (testimony of victims, witnesses, suspects) and virtual (ECT memory, cache memory of Internet service providers servers, smartphone memory, cache memory of the electronic register of the terminal or ATM) of information.

A probable «portrait» of the criminal has been formed. It was found that persons who commit criminal offenses related to the use of e-banking have a high level of intelligence, ingenuity and sociability. A characteristic characteristic of a criminal (hackers, phishers, freakers, spammers, cybersquatters, specialists in software and ECT use) is a special kind of signs – intellectual. These persons possess special knowledge and skills in the field of electronic business, e-commerce, Internet trade, carrying out banking operations, using digital technologies, computer programming, etc. They are mostly men, aged 20-40, who have a basic or complete higher education.

Victimogenic groups of victims are singled out, in particular: a) natural persons who bought and sold goods and services on online platforms and internet auctions using e-banking; b) employees of financial institutions, enterprises and organizations of various forms of ownership; c) their clients; d) relatives of clients; e) legal entities – when carrying out material and technical supply and other

measures in cases of using Internet banking.

Specifics of the initial stage of the investigation of criminal offenses related to the use of e-banking are specified. It has been established that the initial information that became the reason for entering information into the Unified register of pre-trial investigations on the fact of the commission of criminal offenses received by law enforcement agencies.

Typical investigative situations that arise at the initial stage of the investigation of criminal offenses are distinguished: 1) a criminal offense related to the use of e-banking has been committed, a sufficient amount of evidentiary information is available, the identity of the criminal has been established; 2) a criminal offense has been committed, there is a sufficient amount of evidentiary information, the identity of the criminal has not been established; 3) a criminal offense has been committed, there is a sufficient amount of evidentiary information, the identity of the criminal has been established, but criminal actions are disguised as legal financial activity; 4) a criminal offense has been committed, the victim's statement is available, there is no evidentiary information.

The system of tactical tasks that take place in the activities of law enforcement officers in criminal proceedings of the studied category is outlined, as well as a set of measures to solve them within the framework of conducting a number of tactical operations.

A list of questions that must be asked during the questioning of the suspect is proposed, such as: how the illegal actions were committed (contactless – using a public Wi-Fi network, home Wi-Fi network, contact – using an ECT with set passwords) ; what methods were used to enter the e-banking application (use of spam bots; use of card details received from the user or from the sites of fictitious online stores;мapplication of virus programs); during which period the criminal offenses were committed and what accompanying illegal acts were committed; whether illegal actions of OG or CO were committed; if so, what are the functions of each of their participants and what is the system of distribution of funds between them; what means were used during the commission of illegal actions (technical –

ECT, modems, smartphones, routers; software – web browsers, VPN); what was the total amount of money (currency, cryptocurrency) at the time of the completion of the criminal offenses related to the use of e-banking.

The organizational and tactical features of the interaction of the units of the National Police of Ukraine (cyber police, investigations), as well as the forms of interaction, in particular, the implementation of the instructions of the authorized person during investigative (search) actions, secret investigative (search) actions and other measures, the exchange of information, the provision of information to the authorized person, which collected in the process of operational and investigative activities, to resolve the issue of entering information into the Unified register of pre-trial investigations, joint planning of search activities, implementation by the operational unit of the instructions of the authorized person regarding the verification of information that is important for establishing the presence or absence of grounds for entering information into the Unified register of pre-trial investigations based on operational materials.

A list of preventive measures that can be carried out by authorized persons of law enforcement agencies (investigations, inquiries, cyber police) in relation to the elimination of the causes and conditions for committing criminal offenses related to the use of e-banking has been formed, namely: notification of citizens through mass media about legal responsibility (administrative, civil, criminal) for illegal actions; implementation of preventive influence on citizens through the use of separate procedural actions for the purpose of prevention; identification of persons prone to antisocial behavior in the field of use of electronic computing equipment, as well as their further registration in cyber police units; participation of cyber police officers in thematic programs, round tables or talk shows; studying the materials of criminal proceedings to find out and eliminate the conditions and reasons that contributed to the commission of illegal acts; organization of discussions in mass media (electronic and printed), in which cybercrime and its impact on society are discussed; informing citizens in social networks, mass media, messengers about the facts of criminal offenses related to the use of e-

banking (phishing, carding, spamming).

It has been established that one of the main reasons for the ineffectiveness of measures to prevent criminal offenses related to the use of e-banking remains the low level of awareness of investigators and employees of operational units of the National Police regarding typical criminal schemes during the implementation of illegal banking operations and areas of electronic evidence collection. identification of offenders based on a digital trace picture, features of documenting criminal acts in cyberspace, etc.

Proposals have been made regarding the introduction of a rule into the current Code of Criminal Procedure of Ukraine, which will specify the duty of law enforcement officers (investigators, investigators, detectives, prosecutors) to ensure the elimination of the causes and conditions that contributed to the commission of illegal acts.

Tactical operations related to the collection of primary data on the circumstances of the criminal event and the detection of signs of the investigated illegal acts are disclosed, among them the following are defined: «Establishment of the nature of the event of the criminal offense», «Clarification of the place and time of the commission of the illegal act», «Establishment of the method of commission illegal act (phishing, use of spyware, spam bots)», «Identification of the criminal and his accomplices, as well as their search and arrest», «Clarification of the identity of the victim and his victim behavior, as well as verification of their connections» etc.

Based on the generalization of judicial and investigative practice, a list of investigative (search) actions, secret investigative (search) actions and other procedural measures necessary for the effective implementation of tactical operations in criminal proceedings is proposed. Tactical mistakes made by authorized persons during their implementation have been revealed.

A system of measures has been developed for the implementation of the tactical operation «Identification of the criminal and his accomplices, as well as their search and detention», in particular: interrogation of the victims; establishing

and questioning witnesses; review of electronic computing equipment; removal of information from electronic information systems or part thereof; establishing the location of a radio-electronic device; establishing the identity of the criminal and declaring him wanted; establishing the location of the criminal; detention of the criminal; sending requests for the provision of information by law enforcement agencies, state authorities and local self-government bodies, which is important for criminal proceedings on the facts of committing illegal acts related to the use of e-banking; searches at the place of residence and other places of residence of the criminal; questioning of the suspect to identify possible accomplices of the criminal offense; detaining accomplices (members of the OCG who are involved in criminal activity); exchange of information between relevant units of law enforcement agencies of foreign countries and intergovernmental bodies (Interpol, Europol) regarding response to cybercrimes; appointing and conducting forensic examinations.

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

– *legislative activity* – in order to improve the legislation in the field of prevention of criminal offenses related to the use of e-banking, a number of recommendations regarding the introduction of changes and additions to the current Criminal Procedure Code of Ukraine have been laid out;

– *scientific activity* – to improve the methodology of investigation of certain types of criminal offenses against property (implementing acts of the National Academy of Internal Affairs dated 26.02.2024, Kharkiv National University of Internal Affairs dated 29.02.2024, Dnipro State University of Internal Affairs dated 11.03.2024);

– *the educational process* – when teaching the educational disciplines «Organization of the investigation of criminal offenses», «Criminal studies», «Criminal process», «Operational investigative activity», «Forensic means and methods of investigation of criminal offences» as well as the preparation of

textbooks and training manuals (implementation acts of the National Academy of Internal Affairs dated February 27, 2024, the Institute of Law and Public Relations of the Open International University of Human Development «Ukraine» dated March 13, 2024);

– *law enforcement activities* – to improve the activities of pre-trial investigation bodies, operational and expert units of the National Police (acts of the implementation of the Strategic Investigations Department in the Dnipropetrovsk region of the National Police of Ukraine dated September 21, 2023).

Keywords: *e-banking, banking operations, e-business, electronic transfer, transaction, cybercrimes, commerce, internet banking, pre-trial investigation, methodology, forensic characteristics, criminal offense, investigative (search) actions, expertise, special knowledge.*

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано
основні наукові результати дисертації:

1. Малютін Е. В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Т. 2. С. 143–147.

2. Малютін Е. В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Т. 2. С. 122–128.

3. Малютін Е. В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 425–428. URL : http://www.lsej.org.ua/9_2021/9_2021.pdf.

4. Малютін Е. В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія : Право.* 2022. № 2. С. 232–236.

5. Малютін Е. В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

6. Малютін Е. В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 77–82.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Малютін Е. В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

8. Малютін Е. В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

9. Малютін Е. В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права,

2022. С. 139–141.

10. Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146.

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
ЗО	–	Злочинна організація
ІКЕ	–	Інформаційно-комп’ютерна експертиза
ІТ	–	Інформаційні технології
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
ПК	–	Персональний комп’ютер
ПКЕ	–	Програмно-комп’ютерна експертиза
СКТЕ	–	Судова комп’ютерно-технічна експертиза
СОГ	–	Слідчо-оперативна група
СРД	–	Слідча (розшукова) дія
п.	–	Пункт
р.	–	Рік
с.	–	Сторінка (сторінки)
ст.	–	Стаття
ч.	–	Частина

ВСТУП

Обґрунтування вибору теми дослідження. Процес інтеграції України до європейського співтовариства та безперервні зміни у цифровій галузі, що відбуваються в соціумі, впливають на всі сфери суспільного життя. Під час повномасштабного вторгнення російської федерації на територію України суттєво збільшилася кількість кримінальних правопорушень у кіберпросторі. Це переважно протиправні діяння у сфері е-комерції, використання банківських електронних платежів, е-бізнесу та ін. Зважаючи на збільшення чисельності внутрішньо переміщених осіб, релокацію бізнесу зі східних і південних областей країни у її центральні та західні регіони, а також за кордон, спостерігається зростання кількості кримінальних правопорушень, пов’язаних із використанням е-банкінгу, що вчинюються майже в усіх суспільних сферах – від побутової до загальнодержавної. Дедалі спостерігається суттєве збільшення кількості зламів і пошкоджень різноманітних платіжних систем та втручань у їхню ефективну діяльність. До протиправної діяльності залучаються хакери, фахівці у сфері комп’ютерних технологій та програмування, представники кримінальних угруповань, які діють в економічному секторі, адже така діяльність приносить значні злочинні прибутки.

Так, відповідно до офіційної статистичної звітності Офісу Генерального прокурора у 2019 р. до ЄРДР було внесено 2467 фактів шахрайства, учиненого шляхом незаконних операцій із використанням електронно-обчислювальної техніки, а особам вручено повідомлення про підозру лише у 706 випадках. Щодо інших статей КК України, котрі корелюються із застосуванням е-банкінгу, у цей період була майже подібна ситуація, зокрема: за ст. 200 КК України – 711 фактів зареєстровано, з них 674 повідомлення про підозру; за ст. 222 КК України – 76 фактів зареєстровано, з них 59 повідомлень про підозру; за ст. 231 КК України – 8

фактів зареєстровано, повідомлення про підозру відсутні; за ст. 232 КК України – 5 фактів зареєстровано, повідомлення про підозру відсутні; за ст. 361 КК України – 1183 факти зареєстровано, з них 706 повідомлень про підозру; за ст. 361-1 КК України – 191 факт зареєстровано, з них 152 повідомлення про підозру; за ст. 361-2 КК України – 57 фактів зареєстровано, з них 24 повідомлення про підозру; за ст. 362 КК України – 762 факти зареєстровано, з них 598 повідомлень про підозру; за ст. 363^1 КК України – 4 факти зареєстровано, повідомлення про підозру відсутні. У період 2020–2023 рр. значних коливань у статистичних показниках не спостерігалося. У І півріччі 2024 р.: за ст. 200 КК України – 469 фактів зареєстровано, з них 422 повідомлення про підозру; за ст. 222 КК України – 39 фактів зареєстровано, з них 21 повідомлення про підозру; за ст. 231 КК України та ст. 232 КК України відповідно 0 та 1 факт зареєстровано, повідомлення про підозру відсутні; за ст. 361 КК України – 1214 фактів зареєстровано, з них 793 повідомлення про підозру; за ст. 361-1 КК України – 24 факти зареєстровано, з них 3 повідомлення про підозру; за ст. 361-2 КК України – 116 фактів зареєстровано, з них 69 повідомлень про підозру; за ст. 362 КК України – 1001 факт зареєстровано, з них 822 повідомлення про підозру; за ст. 363-1 КК України – взагалі відсутня реєстрація фактів. З огляду на наведені показники злочинна діяльність у сфері використанням е-банкінгу залишається на достатньо високому рівні, а кількість притягнутих до відповідальності осіб дедалі зменшується.

Зважаючи на швидкоплинність інформаційних процесів, неврегульованість низки проблем стосовно функціонування е-банкінгу, низький рівень контролю з боку відповідних державних контролюючих органів, а також суттєве збільшення злочинних посягань у цій сфері, виникає необхідність розробки сучасної дієвої методики розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу.

Крім того, на потребу створення окремої комплексної методики розслідування кримінальних правопорушень, пов’язаних із використанням е-

банкінгу, вказали 92 % опитаних респондентів. З-поміж причин низької якості розслідування зазначених діянь вони вказали такі: неналежне процесуальне керівництво досудовим розслідуванням – 56 %, низький фаховий рівень працівників підрозділів правоохоронних органів, які задіяні у кримінальних провадженнях досліджуваної категорії – 62 %, невчасне проведення слідчих (розшукових) дій, НСРД та інших заходів – 32 %, низький рівень координації взаємодії слідчого з працівниками оперативних підрозділів і кіберполіції – 67 %, небажання потерпілих і свідків співпрацювати з уповноваженими особами – 39 %.

Теоретичне підґрунтя дисертації стосовно різних аспектів розслідування кримінальних правопорушень становлять фундаментальні роботи науковців, а саме: Ю. Аленіна, В. Бахіна, В. Весельського, А. Волобуєва, І. Гори, В. Дарагана, В. Дрозд, М. Єфімова, В. Журавля, А. Іщенка, В. Коновалової, В. Кузьмічова, В. Лукашевича, Є. Лук'янчикова, І. Пирога, М. Погорецького, М. Салтевського, Р. Степанюка, О. Тарасенка, О. Татарова, О. Тіщенка, П. Цимбала, К. Чаплинського, С. Чернявського, Ю. Чорноус, В. Шепітька, М. Щербаковського та ін.

Окремі проблеми розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, досліджували такі вчені, як: Г. Бідняк, С. Буяджи, С. Головкін, А. Жилін, В. Коба, І. Коваленко, Н. Козак, Т. Коршикова, С. Кузьменко, О. Курман, О. Мотлях, О. Мусієнко, Т. Охрімчук, Н. Павлова, В. Пазиніч, Д. Птушкін, Д. Ричка, О. Самойленко, С. Самойлов, В. Хахановський, С. Чернявський, С. Чучко та ін.

З-поміж останніх наукових праць, що стосувалися досліджуваної проблематики, варто виокремити наступні. Так, О. Довженко у дисертації «Основи методики розслідування кіберзлочинів» (м. Харків, 2020 р.) розкрив стан наукової розробки проблем розслідування кіберзлочинів, визначив перелік обставин, що підлягають встановленню у кримінальному провадженні, охарактеризував типові слідчі ситуації, що виникають на початковому етапі розслідування, розглянув особливості допиту

потерпілих, свідків і підозрюваних. У свою чергу, А. Рейнгольд у дисертації «Основи методики розслідування шахрайства в інтернет-комерції» (м. Дніпро, 2023 р.) визначив стан наукового дослідження питань розслідування шахрайства в інтернет-комерції, окреслив специфіку початкового етапу розслідування шахрайства, розглянув основні елементи організації й планування розслідування шахрайства та визначив коло обставин, що підлягають встановленню. А вже В. Сисолятін у роботі «Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» (м. Дніпро, 2024 р.) узагальнив наукові погляди стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та запропонував їх криміналістичну класифікацію; окреслив окремі елементи криміналістичної характеристики протиправних діянь; здійснив криміналістичний аналіз первісної інформації та сформулював коло обставин, що підлягають встановленню у кримінальному провадженні; конкретизував типові слідчі ситуації, що виникають на початковому і подальшому етапах розслідування; з'ясував особливості використання спеціальних знань.

Відзначуючи теоретичну цінність наведених робіт, слід зауважити, що вчені розробляли лише окремі проблемні питання розслідування кримінальних правопорушень визначеної категорії. Недослідженими залишаються питання застосування тактичних операцій щодо збирання первинних даних про обставини злочинної події та виявлення ознак протиправних діянь, координації й взаємодії слідчих та працівників оперативних підрозділів Національної поліції у кримінальному провадженні, не опрацьовувалися питання профілактичної діяльності уповноважених осіб стосовно усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, та ін.

Наведені обставини у своїй сукупності визначили актуальність окресленої проблематики, її теоретичне і практичне значення, а також зумовили вибір напряму дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до положень Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та плану заходів щодо її реалізації (розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 03.03.2021 № 179), Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р), Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України (спільний наказ Офісу Генерального прокурора та МВС України від 22.11.2021 № 371/846), тематики наукових досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022–2026 роки (наказ МОН України від 03.02.2022 № 109), тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11.06.2020 № 454), Основних напрямів наукових досліджень Науково-дослідного інституту публічного права на 2020–2024 рр.

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає у вирішенні конкретного наукового завдання з розробки теоретичних положень та криміналістичних рекомендацій щодо формування методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

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

– визначити сутність та систему криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням е-банкінгу;

– охарактеризувати обстановку та систематизувати типові способи й сліди вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу;

– з’ясувати криміналістично вагомі ознаки особи злочинця, визначити та охарактеризувати віктимогенні групи потерпілих;

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

– розкрити особливості взаємодії слідчих та працівників оперативних підрозділів Національної поліції України у кримінальному провадженні;

– виокремити заходи профілактичної діяльності працівників правоохоронних органів щодо виявлення й усунення причин та умов учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу;

– розкрити тактичні операції щодо збирання первинних даних про обставини злочинної події та виявлення ознак протиправних діянь;

– сформувати перелік заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання».

Об’єктом дослідження є кримінальні процесуальні відносини, що формуються під час функціонування правоохоронних органів при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу.

Предмет дослідження – основи методики розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу.

Методи дослідження. Відповідно до поставленої мети крізь призму об’єкта і предмета дослідження застосовано низку загальнонаукових і спеціальних методів наукового пізнання. *Функціональний метод* використано для формулювання перспективних напрямів застосування тактичних

операцій, а також з'ясування особливостей проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій під час їх реалізації (підрозділи 3.1–3.2). *Системно-структурний метод* було застосовано для формулювання сутності та системи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а також для систематизації типових способів їх учинення та слідової картини (матеріальних, ідеальних, віртуальних слідів) (розділ 1). Використано *документальний метод* для виявлення тактичних помилок і прорахунків в організаційно-тактичному забезпеченні проведення окремих слідчих (розшукових) дій та НСРД (підрозділи 3.1–3.2). *Соціологічний* та *статистичний методи були застосовані* для аналізу судово-слідчої практики, узагальнення статистичних даних, матеріалів кримінальних проваджень і опитування респондентів (розділи 1–3). За допомогою *методу синтезу* зроблено загальні висновки за тематикою дисертаційного дослідження (розділи 1–3).

Емпіричну основу дослідження складають структурована інформація Єдиного звіту про вчинені кримінальні правопорушення Офісу Генерального прокурора України за 2018–2024 рр., а також результати аналізу кримінальних проваджень за 2017–2024 рр. Зокрема, було опрацьовано матеріали 215 кримінальних проваджень із проблематики дослідження у Вінницькій, Дніпропетровській, Донецькій, Закарпатській, Запорізькій, Івано-Франківській, Київській, Львівській, Миколаївській, Одеській, Полтавській, Сумській, Тернопільській, Харківській, Херсонській, Черкаській та Чернівецькій областях та в м. Київ. Також було проанкетовано 250 слідчих, 286 працівників оперативних підрозділів, 52 представники кіберполіції, 96 працівників органів прокуратури, 67 працівників експертних установ МВС України. Крім того, під час проведення дослідження було застосовано власний досвід роботи у підрозділах Національної поліції України.

Наукова новизна одержаних результатів полягає в тому, що дисертаційна робота є першим у вітчизняній науці комплексним

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

вперше:

– запропоновано систему окремої методики розслідування, в яку включено складові з огляду на організаційно-тактичні особливості здійснення кримінальних проваджень, розпочатих за фактом учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, зокрема, додано такі, як: криміналістична характеристика кримінальних правопорушень; розгляд первинної інформації, а також особливості занесення відповідних даних в Єдиний реєстр досудових розслідувань; обставини, котрі варто з’ясовувати під час розслідування; типові слідчі ситуації розслідування; початковий етап розслідування (проведення слідчих (розшукових) дій, НСРД та розшукових заходів); подальший етап розслідування (проведення слідчих (розшукових) дій, НСРД та інших процесуальних заходів); використання спеціальних знань у кримінальному провадженні; тактичні операції; взаємодія підрозділів правоохоронних органів; встановлення причин та умов, що сприяли учиненню протиправного діяння;

– сформовано перелік профілактичних заходів, що можуть проводитись уповноваженими особами правоохоронних органів (слідства, дізнання, кіберполіції) стосовно усунення причин і умов учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, а саме: повідомлення громадян за допомогою засобів масової інформації про юридичну відповідальність (адміністративну, цивільну, кримінальну) за протиправні дії; реалізація профілактичного впливу на громадян шляхом використання окремих процесуальних дій із метою здійснення профілактики;

встановлення осіб, схильних до антисуспільної поведінки у сфері використання електронно-обчислювальної техніки, а також їх подальше занесення до обліку в підрозділах кіберполіції; участь працівників кіберполіції у тематичних передачах, круглих столах або ток-шоу; вивчення матеріалів кримінальних проваджень для з'ясування та усунення умов і причин, що сприяли вчиненню протиправних діянь; організація дискусій у ЗМІ (електронних та друкованих) із обговоренням кіберзлочинності та її впливу на суспільство; інформування громадян у соціальних мережах, ЗМІ, месенджерах щодо фактів учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (фішингу, кардингу, спамінгу);

– розроблено систему заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», як-от: допити потерпілих; встановлення та допити свідків; огляд електронно-обчислювальної техніки; зняття інформації з електронних інформаційних систем або її частини; встановлення місцезнаходження радіоелектронного засобу; встановлення особи злочинця та оголошення її у розшук; встановлення місцезнаходження злочинця; затримання злочинця; направлення вимог щодо надання правоохоронними органами, органами державної влади та органами місцевого самоврядування інформації, що має значення для кримінального провадження за фактами вчинення протиправних діянь, пов'язаних із використанням е-банкінгу; обшуки за місцем проживання та в інших місцях перебування злочинця; допит підозрюваного для встановлення ймовірних співучасників кримінального правопорушення; проведення затримання співучасників (членів ОЗГ, які задіяні до злочинної діяльності); обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерполу, Європолу) стосовно реагування на кіберзлочини; призначення та проведення судових експертиз;

удосконалено:

– теоретичні концепції класифікації типових способів підготовки,

безпосереднього вчинення та приховування протиправних діянь, учинених із використанням е-банкінгу;

– характеристику слідової картини кримінальних правопорушень шляхом надання відомостей стосовно матеріальної (ЕОТ, папілярні візерунки), особистісної (показання потерпілих, свідків, підозрюваних) та віртуальної (пам'ять ЕОТ, кеш-пам'ять серверів інтернет-провайдерів, пам'ять смартфонів, кеш-пам'ять електронного реєстру термінала чи банкомата) інформації;

– систему тактичних завдань, що мають місце у діяльності працівників правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також комплекс заходів для їх вирішення в межах проведення низки тактичних операцій;

– перелік питань, котрі необхідно з'ясовувати під час допиту підозрюваного, як-от: у який спосіб було вчинено протиправні дії (безконтактно – за допомогою мережі Wi-Fi загального користування, домашньої мережі Wi-Fi, контактно – за допомогою заволодіння ЕОТ зі встановленими паролями); які способи використовувалися для входження у застосунок для е-банкінгу (застосування спам-ботів; застосування реквізитів картки, отриманої у користувача або із сайтів фіктивних онлайн-магазинів; застосування вірусних програм); протягом якого терміну були скоєні кримінальні правопорушення та які супутні протиправні діяння було вчинено; чи були вчинені протиправні дії ОГ чи ЗО; якщо так, то які функції кожного з їх учасників та яка система розподілу грошових коштів між ними; які засоби застосовувалися під час вчинення протиправних дій (технічні – ЕОТ, модеми, смартфони, маршрутизатори; програмні – web-браузери, VPN); якою була загальна сума грошових коштів (валюта, криптовалюта) на момент закінчення вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу;

– систему тактичних операцій щодо збирання первинних даних про обставини події та виявлення ознак досліджуваних протиправних діянь, а

саме: «Встановлення характеру події кримінального правопорушення», «З'ясування місця та часу вчинення протиправного діяння», «Встановлення способу вчинення протиправного діяння (фішинг, застосування шпигунських програм, спам-ботів)», «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», «З'ясування особи потерпілого та її віктимної поведінки, а також перевірка їхніх зв'язків»;

дістали подальшого розвитку:

– теоретичні домінанти з приводу загальних кримінально-процесуальних та криміналістичних категорій (як-от: методика розслідування, криміналістична характеристика, обставини, що підлягають доказуванню, типові слідчі ситуації, взаємодія, профілактична діяльність, тактичні операції);

– структура криміналістичної характеристики досліджуваних протиправних діянь, у якій виокремлено такі елементи, як: спосіб та обстановка кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого;

– система відомостей стосовно обстановки вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, крізь призму просторових, часових та соціальних чинників;

– пропозиції стосовно внесення норми в чинний КПК України, в якій буде вказано обов'язок працівників правоохоронних органів (слідчих, дізнавачів, детективів, прокурорів) забезпечувати усунення причин та умов, що сприяли вчиненню протиправних діянь;

– організаційно-тактичні особливості взаємодії підрозділів Національної поліції України (кіберполіції, слідства), а також форми взаємодії, зокрема: здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, НСРД та інших заходів, обмін інформацією, надання уповноваженій особі відомостей, зібраних у процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення інформації до ЄРДР, спільне планування розшукових заходів,

здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, що мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними матеріалами;

– формулювання профілактики протиправних діянь як спеціального різновиду правоохоронної діяльності, що складається із сукупності конкретних дій та заходів, котрі реалізують працівники правоохоронних органів (слідчі, дізнавачі, детективи, прокурори), що має на меті усунення причин та умов скоєння окремих категорій кримінальних правопорушень.

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

– *законотворчій діяльності* – для удосконалення законодавства у сфері попередження кримінальних правопорушень, пов’язаних із використанням е-банкінгу, викладено низку рекомендацій стосовно внесення змін і доповнень до діючого Кримінального процесуального кодексу України;

– *науковій діяльності* – для удосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Національної академії внутрішніх справ від 26.02.2024, Харківського національного університету внутрішніх справ від 29.02.2024, Дніпропетровського державного університету внутрішніх справ від 11.03.2024);

– *освітньому процесі* – при викладанні навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Оперативно-розшукова діяльність», «Криміналістичні засоби та методи розслідування кримінальних правопорушень». а також при підготовці підручників і навчальних посібників (акти впровадження Національної академії внутрішніх справ від 27.02.2024, Інституту права та суспільних відносин Відкритого міжнародного Університету розвитку людини «Україна» від 13.03.2024);

– *правозастосовній діяльності* – для вдосконалення діяльності органів досудового розслідування, оперативних та експертних підрозділів Національної поліції України (акти впровадження Управління стратегічних розслідувань в Дніпропетровській області ДСР Національної поліції України від 21.09.2023).

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.), «Взаємодія публічного та приватного права: сучасні проблеми та виклики» (м. Київ, 2022 р.), «Інноваційні підходи до реформування сучасного законодавства» (м. Київ, 2023 р.).

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

Структура та обсяг дисертації. Дисертація складається з основної частини (вступу, трьох розділів, що містять дев’ять підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 239 сторінок, з яких 159 сторінку – основного тексту. Список використаних джерел налічує 221 найменування і займає 25 сторінок, 4 додатки викладено на 33-х сторінках.

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

1.1. Сутність та система криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу

Методика розслідування окремих видів кримінальних правопорушень вже давно визнана сталою категорією в криміналістиці. В її структурі є низка складових, що, безперечно, завжди до неї входили, як-от: проведення слідчих (розшукових) дій; використання спеціальних знань; типові слідчі ситуації. З іншого боку, є декілька елементів, що базуються на чинному кримінально-процесуальному законодавстві та з його зміною або припиняють своє існування (наприклад, особливості порушення кримінальної справи), або додаються (зокрема, особливості внесення відомостей в Єдиний реєстр досудових розслідувань). Крім того, наявність окремих елементів викликає суперечки між науковцями стосовно їхньої обов'язковості та існування загалом. Із-поміж таких складових особливе місце посідає криміналістична характеристика кримінальних правопорушень, оскільки стосовно її включення в методику розслідування серед учених-криміналістів вже більше ніж півсторіччя виникають проблемні дискусії [112, с. 143].

У цілому слід зазначити, що ми підтримуємо думку В. Журавля, який слушно наголошував на тому, що криміналістична методика виникла в результаті інтеграції та диференціації наукових знань, а також об'єднує в собі передові досягнення криміналістичної техніки й тактики, відповідно, й щодо оптимальної організації розслідування кримінальних правопорушень і судового розгляду певних категорій справ [43, с. 9]. У свою чергу, В. Шепітько зауважує, що методика розслідування окремих видів

кримінальних правопорушень (або криміналістична методика) є важливим розділом науки криміналістики. Також автор надає її формулювання як системи наукових положень і розроблюваних на їх основі рекомендацій щодо організації і здійснення розслідування окремих видів злочинів та запобігання їм. Підсумовуючи, науковець відмічав, що у системі криміналістичних знань згадана методика являє собою синтезуючий рівень, що об'єднує положення криміналістичної техніки і криміналістичної тактики в їх переломленні до умов розслідування певного виду протиправного діяння [85, с. 269].

Інше формулювання досліджуваної наукової категорії надає окрема група дослідників (Б. Лук'янчиков, Є. Лук'янчиков, С. Петряєв), а саме: «…заключний розділ криміналістики, який синтезує положення криміналістичної техніки і тактики та являє собою систему наукових положень та розроблених на їх основі типових рекомендацій з організації розкриття, розслідування і запобігання окремих видів кримінальних правопорушень». Крім того, автори вказують на те, що її «…припустимо розглядати як засіб реалізації положень криміналістичної техніки і тактики. Адже поза реальних умов розслідування відносно особливостей того чи іншого виду злочинів їх застосування неможливо. Так, криміналістична техніка розкриває механізм виникнення слідів рук, але, природно, вона не може дати відповідь, на яких предметах частіше утворюються ці сліди при вчиненні крадіжок або корупційних злочинів. В криміналістичній тактиці розглядають прийоми допиту свідка, але не міститься відповіді на питання, у чому полягають особливості допиту при розслідуванні підпалів, розбійних нападів тощо. Виявлення таких особливостей і є завданням криміналістичної методики. Адже не може бути допиту свідка чи потерпілого взагалі, а є допит конкретних категорій осіб (потерпілих, свідків, підозрюваних) стосовно до специфічних умов, їх ролі, заінтересованості і т. п. в межах розслідування конкретних злочинів» [110, с. 198].

А вже В. Тіщенко зазначає, що загальний метод охоплює всі теоретичні положення криміналістичної методики та спрямовує їх на оптимальне

формування окремих методик і подальшу адаптацію до розслідування конкретного кримінального правопорушення. Крім того, автор відмічає, що вказаний метод не може замінити всі теоретичні положення криміналістичної методики, а з іншого боку, метод слід розглядати як інструмент, спосіб, за допомого якого утворюється окрема методика розслідування, але не фактор, який обумовлює зміст і структуру такої методики. Як висновок науковець вказує, що оптимізація окремих методик розслідування залежить від правильного визначення принципів їх формування у теорії та застосування у практиці [188, с. 115–124].

Зі свого боку, В. Пясковський, Ю. Чорноус та А. Самодін зауважують, що «…назва завершального розділу криміналістики «криміналістична методика» лише умовно передає сутність змістовного навантаження, що охоплює поняття «методика». В криміналістичній методиці розроблюються та рекомендуються до застосування під час розслідування не тільки певні методи, засоби і прийоми діяльності, але й положення, які стосуються: криміналістичної характеристики відповідного виду кримінальних правопорушень; типових слідчих ситуацій; типових переліків обставин, що потребують встановлення; напрямів взаємодії слідчого з іншими учасниками розслідування, правоохоронними та державними органами тощо. Такі рекомендації являють собою програми розслідування за похідною типовою слідчою ситуацією і визначають коло завдань, що вирішуються за допомогою відповідних алгоритмів дій слідчого, тим самим набуваючи технологічного характеру. Криміналістична методика – це завершальний розділ науки криміналістики, що є системою наукових положень і сформованих на їх основі практичних рекомендацій, що забезпечують ефективність діяльності слідчого та інших компетентних суб’єктів з розслідування та попередження окремих видів кримінальних правопорушень» [83, с. 569].

Інша група дослідників (Р. Благута, О. Гумін, Є. Пряхін) визначила досліджувану категорію як «…розділ криміналістики, що становить систему наукових положень і розроблюваних на їх основі рекомендацій щодо

організації і здійснення розкриття, розслідування та запобігання злочинам. У теорії криміналістики існують й інші визначення цього поняття. Відповідно до особливостей розслідування окремих видів злочинів криміналістична методика акумулює в собі засоби і прийоми криміналістичної техніки і тактики» [122, с. 8].

Стосовно наповнення визначеної категорії зауважимо, що, наприклад, В. Шепітько виокремлює такі її типові елементи: «…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» [85, с. 271].

Окрема група вчених-криміналістів із-поміж головних структурних складових зазначеної криміналістичної категорії виокремлює: «1. Криміналістичну характеристику певного виду злочину. 2. Обставини, що підлягають з'ясуванню у справі. 3. Особливості порушення кримінальної справи. 4. Типові слідчі ситуації, типові версії та планування. 5. Першочергові слідчі дії та оперативно-розшукові заходи. 6. Тактику проведення окремих слідчих дій. 7. Профілактичну діяльність слідчого» [122, с. 9–10].

Також вважаємо досить слушною думку М. Єфімова, який вирізняв у структурі методики розслідування окремих видів кримінальних правопорушень такі елементи, як: «…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. 13–14].

Наостанок приведемо позицію М. Салтевського, який серед складових досліджуваної наукової категорії вирізняв такі, як: «…криміналістична характеристика; обставини, що підлягають встановленню; опис типових слідчих ситуацій і відповідні їм програми розслідування; особливості процесу висунення версій і планування дій слідчого на різних етапах розслідування; особливості тактики окремих слідчих (розшукових) дій; специфіка профілактичної діяльності слідчого тощо» [161, с. 133–139].

У підсумку вважаємо за необхідне навести твердження А. Шеремета, який доречно констатує, що «…розроблення методик розслідування спирається на цілісну систему загальних положень (принципів), до яких можна віднести: обумовленість вказаних розробок потребами слідчої практики; реалізація принципу законності наукових рекомендацій, які повинні відповідати принципам кримінального процесу, етичності і гуманності; комплексне використання правових та інших джерел інформації; використання нових досягнень науково-технічного прогресу і передового слідчого досвіду, інших сфер практичної діяльності; оптимальний набір слідчих дій, тобто в будь-якій окремій методиці доцільно використовувати повну сукупність слідчих дій, яка забезпечує вирішення слідчої ситуації, досягнення мети розслідування» [212, с. 336]. А вже Б. Щур вказував, що класифікація окремих методик розслідування кримінальних правопорушень обумовлена тим, що на визначення її складових безпосередньо впливає вид вказаних методик. Зокрема, автор акцентує увагу на тому, що вони повинні сприяти ефективності розслідування відповідних видів (груп) протиправних діянь. Адже, на думку науковця, більшість вчених-криміналістів засвідчує, що завдання методики розслідування полягає у визначенні основних напрямів розслідування певного виду, групи протиправних діянь [213, с. 5].

Як бачимо, всі вищеперераховані науковці підтримують прикладне значення методики розслідування окремих видів кримінальних правопорушень, а також визначають відповідні її складові з огляду на наявні законодавчі та наукові тенденції. На нашу думку, необхідно виокремити такі складові досліджуваної криміналістичної категорії під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу:

– криміналістичну характеристику кримінальних правопорушень;

– розгляд первинної інформації, а також особливості занесення відповідних даних в Єдиний реєстр досудових розслідувань;

– обставини, що їх варто з'ясовувати під час розслідування;

– типові слідчі ситуації розслідування;

– початковий етап розслідування (проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів);

– подальший етап розслідування (проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів);

– використання спеціальних знань у кримінальному провадженню;

– тактичні операції;

– взаємодію підрозділів правоохоронних органів;

– встановлення причин та умов, що сприяли вчиненню протиправного діяння.

В розрізі зазначеного вважаємо за потрібне охарактеризувати наукові підходи стосовно сутності окремих наукових категорій, що характеризують правовідносини у сфері використання банківських електронних платежів, як-от: «електронна торгівля», «е-банкінг», «цифрова торгівля», «е-бізнес», «е-комерція» тощо, котрі відрізняються і мають різний зміст та наповнення.

Ми підтримуємо позицію групи дослідників (К. Крауса, Н. Крауса, О. Манжури), які вказують, що концепція е-бізнесу виникла у США ще у 80-х роках XX ст. та стала результатом розвитку ідеї глобальної інформаційної економіки, що була теоретичною основою створення локальних і корпоративних інформаційних мереж із поєднанням застосування

інформаційних технологій у компаніях. Крім того, автори відмітили, що термін «е-комерція» тотожний поняттю «електронна комерція (торгівля) та цифрова торгівля». У той час як е-бізнес – це складова е-комерції нарівні з інфраструктурою ІТ. І навпаки – е-комерція є такою, що становить е-бізнес, це один зі способів його здійснення [80, с. 18, 20].

Важливим елементом у зазначеній структурі є криміналістична характеристика кримінальних правопорушень. Вбачаємо досить слушною думку Т. Вискарки, яка з приводу зазначеної наукової категорії вказувала, що та «…є відносно новою категорією в сучасній криміналістиці, оскільки перші згадки про неї почалися лише в сімдесятих роках минулого сторіччя. Найбільшого розквіту її дослідження на теренах української науки почалося приблизно з 2010 року. Саме тоді майже всі вчені-криміналісти при висвітленні питань окремих методик розслідування кримінальних правопорушень вважали за необхідне розглянути і вказану складову. Як наслідок, зазначена категорія стала невід'ємною частиною будь-якої окремої методики» [23, с. 106].

Стосовно формулювання вказаної криміналістичної категорії слід зазначити, що, наприклад, окрема група науковців визначила її як «…систему відомостей про криміналістично значущі ознаки злочинів цього виду. Вона відображає закономірні зв'язки між цими ознаками і сприяє побудові та перевірці слідчих версій, що висуваються в процесі розслідування злочинів. Криміналістичну характеристику можна уявити як ідеальну модель типових зв'язків та джерел доказової інформації, що дозволяють спрогнозувати оптимальний шлях і найбільш ефективні засоби розслідування окремих категорій злочинів» [122, с. 10]. А вже В. Пясковський, Ю. Чорноус та А. Самодін сформулювали поняття досліджуваної наукової категорії як систему узагальнених даних про найбільш типові ознаки певного виду (групи) кримінальних правопорушень, закономірний взаємозв'язок яких слугує основою наукового і практичного вирішення завдань розслідування [83, с. 579].

Зі свого боку, В. Лисенко щодо значення криміналістичної характеристики зауважував, що вона «…має практичне призначення не лише у випадку встановлення типових зв'язків між її елементами. Вона може бути також ефективно застосована у діяльності слідчих органів за наявності нетипових особливостей окремих елементів чи зв'язків. Виходячи з наведеного, можна зазначити, що до змісту криміналістичної характеристики необхідно включати інформацію про злочини, яка має одиничні прояви. Такі нетипові прояви злочинної діяльності можуть мати поширення у майбутньому» [104, с. 234]. Інша група науковців наголошує, 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» [110, с. 209]. Також вважаємо досить цікавим визначення В. Бахіна та Б. Лук'янчикова, які надали таке формулювання: криміналістична характеристика злочинів – це система узагальнених даних про найбільш типові криміналістично значущі ознаки певного виду злочинів [5, с. 40].

Підсумовуючи, сформулюємо власне визначення досліджуваної наукової категорії: це система взаємопов'язаних відомостей про криміналістично значущі ознаки кримінального правопорушення, що поєднані відповідними кореляційними зв'язками та допомагають у розслідуванні завдяки побудові версій у результаті проведення окремих процесуальних дій та розшукових заходів.

Наповнення відповідними елементами криміналістичної характеристики різних категорій кримінальних правопорушень викликає наукові дискусії серед вчених-криміналістів. Тому вважаємо за необхідне зупинитися на наповненні складовими вказаної наукової категорії під час розслідування кримінальних правопорушень, пов'язаних із використанням е-

банкінгу.

Стосовно досліджуваної групи протиправних діянь загалом О. Селезньова слушно зауважує, що «…немає потреби вважати інформаційні правовідносини такими, які створюються тільки в інформаційній сфері, оскільки розглядувані відносини можуть виникати і в інших сферах життєдіяльності, наприклад, у сфері цивільно-правового обороту, коли певний об’єкт інформаційних відносин стає предметом цивільного договору» [172, с. 212].

З-поміж елементів криміналістичної характеристики окрема група науковців (В. Пясковський, Ю. Чорноус, А. Самодін), наприклад, називає такі, як: «…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, розподіл 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)» [83, с. 580].

А вже А. Волобуєв, О. Одерій та Р. Степанюк зазначають такі складові

вказаної наукової категорії: «…предмет злочину (гроші, матеріальні цінності, наркотичні речовини тощо); місце, час та обстановка, характерні для вчинення злочинів окремих видів; способи підготовки, вчинення та приховування злочинів – певна система дій, прийомів та окремих операцій злочинців, у т.ч. використання знаряддя злочину (автотранспорту, вогнепальної й холодної зброї, знарядь зламу, обладнання для виготовлення фальшивих документів тощо); сліди злочинів (різноманітні зміни, які вносяться ними в навколишню обстановку); особа злочинця (комплекс властивостей злочинця, його зв'язків і відносин, пов'язаних з учиненням злочинів, що можуть бути використані для їх розслідування); особа потерпілого (характер поведінки, майнове положення, соціальні зв'язки тощо)» [86, с. 9].

Зі свого боку, Н. Карпов визначив таке наповнення криміналістичної характеристики: «…спосіб вчинення злочину; місце і обстановка; час вчинення злочину; знаряддя і засоби; предмет посягання; потерпіла особа; особа злочинця; сліди злочину (у широкому значенні)» [58, с. 268–269].

У свою чергу, Т. Охрімчук так формулює склад криміналістичної характеристики шахрайства з фінансовими ресурсами: «…спосіб вчинення; слідова картина шахрайства з фінансовими ресурсами; особа шахрая з фінансовими ресурсами» [132, с. 373]. У розрізі зазначеного вважаємо за потрібне навести визначення поняття «фінансове шахрайство», сформульоване Ю. Хамигою, як «сукупності економічних відносин, які реалізуються юридичними або фізичними особами (як правило, без насильницьких дій) у процесі формування, розподілу і використання фінансових ресурсів (доходів) шляхом обману або зловживання довірою чи службовим становищем з метою отримання економічної та/або іншої вигоди (особистої, корпоративної чи на користь третіх осіб), в результаті яких відбувається отримання економічних вигід шахраєм та збитків – жертвою шахрайських дій. Такий підхід, на відміну від наявних, системно і всебічно розкриває сутність фінансового шахрайства та акцентує увагу передусім на

фінансових аспектах цього поняття, конкретизації мети, способів та наслідків фінансового шахрайства, а також дає можливість сформувати комплекс заходів щодо попередження і мінімізації фінансового шахрайства як цілісної системи, спроможної докорінним чином вплинути на подолання цього суспільно-небезпечного явища» [218, с. 8].

З огляду на дослідження криміналістичної характеристики правопорушень, пов'язаних із використанням е-банкінгу, наведемо твердження І. Коваленка, який зауважує, що «…якість та результативність розкриття протиправних діянь в сфері банківських електронних платежів прямо пропорційно залежить від професійного рівня ІТ-фахівця, наявності передових технологій у правоохоронних органах та швидкості реагування на дії кіберзлочинців. Криміналістична характеристика визначених протиправних діянь містить наступні елементи: спосіб учинення шахрайства, обстановку вчинення кримінального правопорушення, слідову картину, особу шахрая та особу потерпілого» [67, с. 367].

Також вважаємо за потрібне наголосити на тому, що купівля-продаж товарів і послуг між суб'єктами у мережі Інтернет здійснюється за допомогою низки платформ. Зокрема, В. Капцош опрацював дії таких платформ у власному дослідженні та відмітив, що «…створення власного сайту дає змогу повноцінно представити себе в Інтернеті, максимально розповісти про свою компанію і товари споживачу, розвивати товарну марку, виділитися серед конкурентів, відстежити дії відвідувачів. Проте розроблення сайту інтернет-магазину – це лише початковий етап. Щоб забезпечити обсяги продажу, необхідно просувати сайт у пошукових системах, удосконалювати його структуру та контент. Електронні дошки оголошень – це веб-сайти для зберігання та публікації оголошень, де кожен бажаючий може викласти свою рекламну інформацію. Для зручності використання такого майданчика віртуальна дошка оголошень зазвичай поділена на розділи згідно з тематикою оголошень. Рекламна публікація на дошці оголошень може бути як платною, так і безкоштовною. Як правило, це

впливає на рейтинг реклами на сайті. Як самостійний спосіб продажів дошки оголошень можуть бути цікаві лише приватним особам для одноразових операцій, здебільшого продажу вживаних товарів. Наступною платформою є соціальні мережі, що набирають свою силу як інструмент маркетингу для багатьох галузей торгівлі. Їх використовують як підприємці-початківці для створення нового бізнесу, так і великі компанії для формування додаткового каналу збуту або забезпечення зв'язків із громадськістю. Однак у цього способу збуту продукції є певні обмеження. Ступінь успішності продажів залежить від унікальності продукту. Чим більш стандартизованим є товар, тим складніше його продавати, тим більше дисконт, який необхідно запропонувати покупцю. Через наявність високого ризику ціна продукту є дуже вагомим фактором. Торгові центри – це платформи для продажів товарів і послуг в Інтернеті, що об'єднують тисячі компаній з різних галузей бізнесу. Здебільшого продавцями на цьому сегменті інтернет-ринку є компанії, а не приватні особи. Загалом цей спосіб збуту в Інтернеті є досить ефективним, але він має низку недоліків порівняно з власним інтернет-магазином. Одним з них є щорічна плата за публікацію сайту на платформі, що часом дорівнює витратам на створення власного інтернет-магазину з більш широкими функціональними можливостями, індивідуальним дизайном, не говорячи вже про можливості переходу на сайт магазину в пошукових системах» [56, с. 115].

Інший автор, О. Курман виділяв такі елементи криміналістичної характеристики шахрайства з фінансовими ресурсами: «…способи вчинення шахрайства з фінансовими ресурсами, обстановка вчинення злочину, особа злочинця, сліди злочину» [101, с. 200]. У свою чергу, Т. Коршикова наголошує на тому, що «…наразі є об'єктивна потреба в узагальненні та впорядкуванні наявних методичних рекомендацій щодо розслідування шахрайств, учинених з використанням ЕОТ, з метою формування комплексної криміналістичної методики. Об'єднані в єдиній класифікаційній групі ідеї і теоретичні положення стають цілісною теоретичною концепцією.

В основі цієї концепції – характеристика різних видів кримінальних правопорушень, урахування якої дозволяє об'єднати окремі рекомендації в єдину методику. До допоміжних компонентів цієї концепції відносимо положення криміналістичної» [75, с. 41].

Зі свого боку, С. Самойлов виокремив складові криміналістичної характеристики шахрайств, учинених із використанням мережі Інтернет, як-от: «…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» [169, с. 21].

Окрема група науковців (М. Комаров, С. Гончар, А. Ониськова) на основі проведеного аналізу та дослідження нормативних документів наголосила на можливості «…визначити основні складові частини систем захисту інформації об'єктів критичної інфраструктури, сформулювати основні завдання із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави, визначити основні напрямки забезпечення інформаційної безпеки об'єктів критичної інфраструктури, показати, що важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу, виділити основні етапи створення систем захисту інформації на об'єктах критичної інфраструктури держави, визначити склад таких систем захисту» [73, с. 47].

Наостанок наведемо твердження М. Комарова, який вказував: «…кількість комп'ютерних атак, що постійно збільшується, призводить до необхідності створення організованих (або таких, що здатні самоорганізовуватись) структур, які призначені для забезпечення та надання актуальної інформації про виявлені кіберзагрози, кібератаки та кібервразливості системи, їх оперативне усунення, створення систем виявлення та запобігання вторгнень, та інших заходів. З цієї причини існують дуже великі масиви інформації щодо актуальних комп'ютерних атак та вразливостей комп'ютерних мереж та систем. Однак часто ця інформація

(особливо, що стосується атак) є дуже різнорідною, неструктурованою та мало придатною для подальшого аналізу. Як наслідок, в даному випадку виникає необхідність в розробці моделі та інструментарію, які за своїм призначенням направлені на можливість упорядкування та систематизації накопичених знань. Іншими словами – створення таксономії. Крім змістовного і систематичного опису комп'ютерних атак, на практиці таксономія атак потрібна для їх подальшого аналізу з метою акумулювання знань при оцінці ризиків і створення моделей загроз та моделей порушника на етапах проектування критично важливих систем, в тому числі інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури. А також для розробки політики безпеки та, зрештою, для створення засобів активного аудиту» [72, с. 29].

У підсумку зазначимо, що нами вирізнено такі складові криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу: спосіб і обстановку вчинення кримінального правопорушення, слідову картину, особу злочинця, особу потерпілого [115, с. 146]. Також вважаємо, що наведені елементи повинні бути максимально оптимізовані й спрямовані на вирішення практичних завдань кримінального провадження. Крім того, зазначені складові мають сталі кореляційні зв'язки та важливе значення для початкового етапу розслідування з огляду на можливість висунення слідчих версій та проведення невідкладних СРД та НСРД.

1.2. Спосіб учинення кримінального правопорушення як основний елемент криміналістичної характеристики

Криміналістична характеристика нараховує низку елементів, кожен із яких, з огляду на конкретне протиправне діяння, буде мати своє значення. На нашу думку, для кримінальних правопорушень, пов'язаних із використанням

е-банкінгу, найбільш важливе значення з усіх складових згаданої наукової категорії буде мати спосіб їх учинення. Оскільки зазначений елемент породжує утворення багатьох кореляційних зв'язків, як-от: «спосіб учинення» – «особа злочинця»; «спосіб учинення» – «особа потерпілого»; «спосіб учинення» – «слідова картина». Адже саме спосіб учинення впливає на всі інші елементи: особа злочинця обирає той спосіб, що найбільш їй притаманний; особа потерпілого стає жертвою, позаяк їй притаманні певні риси, котрі зумовлюють використання відповідного способу вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу. Тому вказаний елемент криміналістичної характеристики потребує детального опрацювання [120, с. 77].

Одразу наведемо тезу Н. Павлової, яка зауважила, що вказана складова є центральною та визначальною, за допомогою якої «…можна дослідити виявлені у процесі аналізу зв'язки між всіма структурними елементами криміналістичної характеристики злочину» [136, с. 20]. У цьому розрізі вважаємо досить доречною позицію В. Тищенка, який в системі способу вчинення протиправного діяння виокремлює «…комплекс діянь злочинця з підготовки, вчинення і приховування злочину, обумовлених метою злочинного діяння, властивостями особи злочинця й обстановкою (об'єктивними і суб'єктивними факторами), результати яких відбиваються на матеріальних та інтелектуальних слідах, що характеризують психічні й фізичні риси особи злочинця» [186, с. 18].

Зі свого боку, В. Білоус із приводу повноструктурності складу кримінального правопорушення відмічає, що «…під час готування до злочину, при вчиненні злочину і після нього особа керується логікою досягнення злочинного результату та уникнення відповідальності. Злочинець, маючи наміри приховати злочин, ретельно обмірковує спосіб його вчинення з тим, щоб надійно приховати сліди злочину. Крім вибору місця і часу вчинення злочину, підготовка до нього включає визначення: а) способу вчинення злочину; б) знарядь злочину; в) способу приховування

(дійсного приховування і притворної поведінки, що відображає позицію, обрану злочинцем); г) способу приховування слідів. Таким чином, злочинець уявно формулює модель майбутньої події, реальне втілення якої буде залежати від ситуації, що об'єктивно складеться. Моделювання включає і варіанти зміни намірів і злочинної поведінки у випадку, якщо обрана схема не може бути реалізована» [12, с. 40].

Також вбачаємо слушним твердження В. Журавля стосовно того, що «…функціональний аспект поведінки злочинця обраний для характеристики способу вчинення злочину як системи дій, прийомів, операцій, що спрямовані на досягнення певного злочинного результату. 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 злочину – до способу вчинення злочину; від способу вчинення злочину – до особи злочинця» [44, с. 28].

А вже О. Кривопуск наголошує на тому, що «…спосіб скоєння злочину дає найбільший обсяг криміналістичної інформації, який в подальшому допомагає слідчому, прокурору, суду чи іншим посадовим особам правоохоронних органів визначити найбільш ефективні методи, спрямовані на розкриття та розслідування злочину, дасть змогу слідчому висунути необхідні версії та ініціювати проведення необхідних слідчих (розшукових) дій, визначити правильний порядок та послідовність їх проведення» [81, с. 370]. В розрізі наведених позицій вважаємо досить правильною думку С. Зав'ялова, який зауважує, що визначена криміналістична категорія корелюється з іншими елементами криміналістичної характеристики так: «…різновид діяльності людини, якій притаманні соціально-психологічні якості, орієнтувальні, сенсомоторні особливості суб'єкта» [45, с. 5].

У свою чергу, Т. Дубно зазначає, що «…спосіб вчинення злочину пов'язує ще й з фізичними та функціональними можливостями людини, що

обумовлюються характером вчинюваного злочину та зовнішніми умовами» [30, с. 226]. Інша група авторів (В. Весельський, С. Зав'ялов, В. Пясковський) зазначену категорію характеризують як «…спосіб дій з готування, вчинення та приховання слідів злочину, що характеризує криміналістично значимі відомості про виконавця і застосовані ним засоби та можливості їх використання у розкритті та розслідуванні злочинів» [22, с. 27]. Як бачимо, всі вищенаведені дослідники формулюють обов'язкове поєднання трьох елементів способу: підготовки, безпосереднього вчинення та приховування протиправного діяння.

З приводу окремих кримінальних правопорушень, то, наприклад, Г. Бідняк крізь призму розслідування шахрайства сформулювала спосіб його вчинення як «…цілеспрямовані дії з підготовки, безпосереднього вчинення та приховування злочину, які обираються залежно від сфери застосування, мають інтелектуальний характер та об'єднані єдиним задумом, спрямовані на заволодіння чужим майном чи правом на таке шляхом обману чи заволодіння довірою» [9]. Зі свого боку, опрацьовуючи проблематику розслідування шахрайства з фінансовими ресурсами, Т. Охрімчук вказала, що головним елементом його криміналістичної характеристики є спосіб вчинення, що нараховує сукупність взаємопов'язаних дій стосовно підготовки, вчинення та приховування слідів протиправного діяння [133, с. 95].

Вважаємо досить слушною думку А. Рейнгольда, який вказував, що способи шахрайства в інтернет-комерції виявляються у системі взаємопов'язаних дій із підготовки, безпосереднього вчинення та приховування кримінального правопорушення. Автор відмічає, що зазначений факт можна пояснити складним механізмом здійснення правочинів у дистанційному варіанті. Крім того, дослідник акцентує увагу, що протиправні дії можуть розпочатися з розміщення оголошення про продаж певних товарів і послуг, створення фіктивних сайтів, крадіжки персональних даних тощо, а закінчитися отриманням грошей від потерпілих в обмін на «неіснуючі товари» чи «неіснуючі послуги». Підсумовуючи,

науковець констатує, що залежно від кінцевої мети протиправні дії можуть припинятися на певному етапі [154, с. 76].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було встановлено, що повноструктурний склад способу вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, мав місце у 100 % діянь. Адже майже в усіх випадках наявними є елементи підготовки та приховування кримінально караного діяння. Тобто злочинці завжди готувалися до вчинення протиправного діяння та здійснювали дії щодо приховування його результатів.

Отже, спочатку розглянемо підготовку до вчинення протиправного діяння. Наприклад, К. Заяць зауважив, що «…навіть у рамках відкритого кримінального провадження дуже складно сформувати систему доказів наявності злочинного наміру в діях шахрая. Адже, на відміну від інших злочинів, вони відбиваються не стільки в матеріальних слідах, скільки в актах інтелектуального характеру: повідомленні неправдивої інформації, використанні фіктивних документів, маскуванні афери законними рішеннями уповноважених осіб та багатьма іншими» [49, с. 207]. А вже О. Баланюк навів перелік можливих заходів підготовчого характеру, як-от: «…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)» [4, с. 195–196]. Тобто маємо досить широкий перелік можливих дій підготовчого характеру.

У свою чергу, окрема група науковців слушно вказала на те, що «…дії, які вчиняються при шахрайствах, пов'язаних із передачею товарів та грошей в Інтернеті, можна умовно поділити на два «сценарії»: за першим – покупець сплачує вартість лоту, але отримує товар незадовільної якості (товар не відповідає описаному у характеристиці до лоту за кількісно-якісними характеристиками), отримує не той товар або зовсім його не отримує – «шахрайства з боку продавця»; за другим – продавець висилає товар, а кошти за нього не отримує (повністю або частково) – «шахрайства з боку покупця». При шахрайстві з боку покупця при отриманні товару особа не сплачує вартість товару повністю або частково. При шахрайствах з боку продавця, враховуючи те, що описання до лоту, що виставляється на торги, робиться самостійно особою, що його виставляє (продавцем), шахрай свідомо та навмисно вносить в його описання такі характеристики, що не відповідають дійсності (кількість, якість, матеріали виготовлення тощо). Нерідко, визначивши спосіб оплати і отримання грошей, шахраї просто не висилають товар чи висилають той товар, що не відповідає лоту» [15, с. 155].

Стосовно підготовчого етапу до вчинення шахрайств, учинених із використанням електронно-обчислювальної техніки, Т. Коршикова вирізняє такі дії: «…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)» [76, с. 132]. У розрізі викладеного вважаємо за необхідне вказати на особливості створення інтернет-магазинів. Зокрема, Р. Царьов

зауважує, що зазначений процес «…взагалі умовно розділяється на 6 етапів. На першому етапі створення Інтернет-магазину підприємцю необхідно визначити: що він буде продавати, наскільки цей товар підходить для торгівлі через Інтернет. Ідеальний об'єкт для Інтернет-торгівлі – це стандартні не швидкопсувні товари з гарантованими споживчими властивостями. Не будь-який товар може бути реалізований через мережу Інтернет, так, певні товарні категорії мають специфічні обмеження для торгівлі в Інтернеті: одяг і взуття вимагають приміряння, ліки й продукти – термінової доставки й т.п. На другому етапі здійснюється оцінка конкурентів – аналіз сайтів, що пропонують такі ж або аналогічні товари або послуги. На третьому етапі визначається, якими функціями повинен володіти Інтернет-магазин. На четвертому етапі здійснюється розробка технічного завдання на створення Інтернет-магазину. Цей процес повинні здійснювати професіонали в області інформаційних технологій (IT), добре знайомі зі специфікою діяльності компанії. Технічне завдання повинне описувати (визначати) структуру Інтернет-магазину, його дизайн, принципи роботи та розташування інформації. На п'ятому етапі здійснюється вибір необхідного програмного забезпечення для реалізації Інтернет-магазину та безпосередньо сама реалізація проекту. На шостому етапі відбувається розміщення сайту магазину у мережі Інтернет. Існуючі варіанти розміщення сайту: на власному сервері, при цьому він або розташовується у комп'ютерній мережі провайдера за відповідну абонентську плату, або підключається до провайдера за виділеною лінією; на устаткуванні провайдера (віртуальний сервер), у цьому випадку у провайдера орендується дисковий простір (хостінг)» [193, с. 39].

Інша група дослідників із-поміж підготовчих заходів до вчинення кримінальних правопорушень у сфері електронно-обчислювальної техніки виділила такі: «…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)» [84, с. 867]. А вже С. Чучко зазначав, що «способи підготовки до шахрайства, що вчиняється від імені вигаданих осіб, мають дещо спрощений вигляд: визначення найменування товару, що пропонуватиметься для продажу, створення його характеристик та отримання презентабельних фотографій; реєстрація та створення облікового запису особи в інформаційній телекомунікаційній системі під вигаданими анкетними даними; розміщення даних про товар; створення рівня довіри у покупців шляхом здійснення успішних цивільно-правових дистанційних угод та заповнення шкали позитивних оцінок; створення «окремої» електронної адреси для здійснення листування із потенційним споживачем; придбання «окремого» телефонного номеру для здійснення переговорів із потенційним споживачем; вибір способу здійснення розрахунків; реєстрація «електронних гаманців» у відповідних сервісах або отримання платіжної картки для перерахування грошей тощо» [206, с. 235–236].

У свою чергу, А. Жилін, опрацювавши анкетування респондентів, дійшов висновку, що мали місце такі підготовчі дії до вчинення шахрайства у сфері використання банківських електронних платежів: «підбір та підготовка певної електронно-обчислювальної техніки (ноутбук, комп’ютер, планшет тощо); розробка програмного забезпечення, необхідного для вчинення окремих видів шахрайства (фішинг, кардінг); вибір об’єкта шахрайських дій; вибір кола осіб, стосовно яких будуть вчинені шахрайські дії» [41, с. 90].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було встановлено такі підготовчі заходи до вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу:

1) знаходження потрібної електронно-обчислювальної техніки (ноутбуків, комп’ютерів, планшетів);

2) підготовка слушних обставин для реалізації протиправних дій та ін.;

3) виготовлення шпигунських технічних або програмних засобів для

протиправного використання під час здійснення операцій е-банкінгу;

4) збут чи розповсюдження без необхідного дозволу мережею Інтернет відомостей, що мають значення під час здійснення операцій е-банкінгу.

Так, 21.03.2022 гр. Г. о 13 год. 06 хв., використовуючи власний мобільний термінал, розмістив на сайті «OLX» оголошення про надання послуг щодо оренди квартири в м. Івано-Франківськ. Після цього 21.03.2022 за відповідним номером телефону, зазначеним в оголошенні, із ним зв'язався потерпілий гр. Й. У ході спілкування у месенджері «Вайбер» під надуманим приводом шахрай попрохав у потерпілого грошові кошти в сумі 1500 грн., нібито як завдаток за здачу йому в оренду своєї квартири. При цьому шахрай запевнив гр. Й. в тому, що він здає в оренду власне помешкання, хоча такого наміру він не мав. Оскільки потерпілий не підозрював про справжні наміри гр. Г., він цього самого дня, перебуваючи у м. Івано-Франківськ, скориставшись послугами інтернет-банкінгу «ПУМБ online», перерахував шахраю на банківську картку грошові кошти, а саме: 21.03.2022 о 20 год. 11 хв. – 750 грн. та о 20 год. 13 хв. – 750 грн, на загальну суму 1500 грн. [179]. Як бачимо, шахрай виконав низку підготовчих дій: підготував необхідну ЕОТ – власний мобільний термінал; підготував слушні обставини для реалізації протиправних дій – розмістив на сайті «OLX» оголошення про надання послуг щодо оренди квартири в м. Івано-Франківськ.

Переходячи до опрацювання безпосереднього способу вчинення досліджуваної категорії протиправних діянь, зауважимо таке. Зокрема, С. Зав'ялов вказував, що «…реалізація сформованого злочинного наміру, що втілюється в окремих практичних діях суб'єкта, займає велику частину способу вчинення злочину» [46, с. 37]. А вже С. Самойлов запропонував таку класифікацію шахрайських дій, вчинених за допомогою мережі Інтернет: «…а) шахрайства, які пов'язані із купівлею/продажем у мережі «Інтернет»; б) шахрайства, сутність яких полягає в отриманні коштів (майна) шляхом надсилання листів чи повідомлень; в) шахрайства, які для заволодіння

коштами (майном) потребують розробки та розміщення в мережі «Інтернет» дублікатів або вузькоспеціалізованих сайтів для надання псевдопослуг; г) шахрайства, які спрямовані на отримання персональних (реєстраційних) даних (так званий «фішинг»); д) шахрайства, пов'язані з обігом електронних грошей; є) шахрайства, для вчинення яких використовується спеціалізоване та/чи шкідливе програмне забезпечення; е) «комбіновані способи» шахрайств» [167, с. 106].

Зі свого боку, С. Чучко визначив достатньо великий перелік дій щодо протиправних діянь в інтернет-комерції, зокрема: «…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; кібер-втручання в обліковий запис сумлінного продавця, рівень довіри якого відповідає потребам споживачів, та здійснення шахрайських угод від його імені; отримання грошей за лот, виставлений на інтернет-аукціоні, від декількох покупців відразу; отримання грошей за фальсифікований чи заздалегідь зіпсований товар; отримання грошей за товар, що повинний складатися з великої кількості вузлів та комплектуючих без надання всієї складової частини (за умов, якщо це заздалегідь сплановано); шахрайські дії від імені несправжнього «покупця» шляхом отримання ним інформації про номер карткового рахунку, персональні дані та номер мобільного телефону продавця «під легендою» необхідності перерахування грошей з подальшим зняттям з рахунку всіх коштів; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати» [206, с. 237].

У свою чергу, М. Бояджян та Г. Яровенко відмічали, що «…на сьогоднішній день найбільш поширеними видами шахрайських операцій з банківським картками є: скімінг – викрадення інформації з магнітної стрічки картки або ПІН-коду за допомогою спеціальних пристроїв; трапінг –

встановлення пасток на шатер банкомату; фізичне пошкодження банкоматів; фішинг – шахрайство за допомогою Інтернету; вішинг – шахрайство за допомогою мобільного зв'язку; вірусні та хакерські атаки тощо» [215, с. 838].

Також доречною вважаємо позицію С. Чернявського, який зауважує, що «…дослідження способів учинення шахрайств шляхом незаконних операцій з використанням ЕОТ виступає своєрідним «ключем» до описання інших значущих елементів криміналістичної характеристики» [199, с. 9]. В розрізі зазначеного В. Сисолятін окреслив такий перелік способів безпосереднього вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу: «…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.» [175, с. 154].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було визначено, зокрема, такі безпосередні способи вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу:

1) протиправні дії при застосовуванні е-банкінгу;

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

3) протиправні дії з відомостями, що знаходяться в пам'яті електронно-обчислювальної техніки;

4) поширення шпигунських програмних чи технічних засобів, а також їх збут із застосовуванням мережі Інтернет.

Наприклад, 23.03.2020 в період часу з 02 год. 30 хв. до 07 год. 30 хв. гр. Є., знаходячись у квартирі, шляхом незаконних операцій із використанням ЕОТ, маючи достатній рівень технічних та комп'ютерних знань, за допомогою власного комп'ютерного обладнання, шляхом використання спеціалізованого шкідливого програмного забезпечення під назвою «xiaomichecker» та «restart», командні файли яких знаходяться на вказаному комп'ютері, отримав персональні данні потерпілої гр. Я., а саме номер телефону та пароль для входу до її акаунта, які надалі використав для входу в автоматизовану систему е-банкінгу «Приват24» (що є одним із каналів дистанційного обслуговування клієнтів банку і містить інформацію про клієнта, що є достатньою для його ідентифікації). Після чого, діючи умисно, з корисливою метою та мотивом, несанкціоновано, тобто самочинно, без дозволу держателя спеціального платіжного засобу або уповноваженої особи, втрутився у роботу банківської автоматизованої системи та здійснив несанкціоноване втручання в роботу автоматизованих систем, що призвело до витоку та підробки інформації, та в подальшому виконав підробку документа на переказ, котрий існує в електронній формі, а саме – заявки на переказ грошових коштів, після цього використав вказаний підроблений документ на переказ для отримання доступу до банківської картки, виданої на ім'я потерпілої, та безготівковим платежем перевів кошти в розмірі 58 000 грн. [178]. Тобто правопорушник використав шпигунське програмне забезпечення, а також незаконні дії при застосуванні е-банкінгу.

Стосовно способу приховування протиправних діянь М. Салтевський слушно відмічає, що він «…реалізується тоді, коли злочин вчинений, у багатьох випадках зареєстрований і щодо нього ведеться розслідування. Усе це докорінно перебудовує систему його детермінуючих факторів. Коло можливих дій суб'єкта значно розширюється і може включати обмову, неправдиві показання, залякування свідків, наклеп, підробку документів

тощо. У злочинах, учинених у співучасті, спосіб учинення може бути один, а способи приховування – різні в кожного співучасника» [161, с. 426].

У свою чергу, І. Коваленко з приводу особливостей приховування шахрайства у сфері використання банківських електронних платежів констатує, 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» [64, с. 146]. Інший дослідник, А. Рейнгольд із-поміж способів приховування шахрайства в інтернет-комерції вирізнив такі: «…виготовлення і використання фіктивних документів при реєстрації на сайті – 22 %, маскування шахрайських дій під легальні цивільно-правові угоди – 24 %, знищення електронних документів, що використовувалися при здійсненні електронних правочинів – 45 %, знищення персональної інформації, що надавалася провайдеру для реєстрації – 38 %, підкуп свідків – 34 %, маскування зовнішності під час онлайн-спілкування з потенціальною жертвою – 17 %, використання чужих платіжних карток для здійснення грошових переказів – 66 % та ін.» [155, с. 14].

Зі свого боку, А. Жилін виділяв такі заходи приховування досліджуваної категорії шахрайств: «…застосовування трансформації ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються шахрайські дії; надання неправдивих показань при проведенні окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів; ліквідація устаткування, що засовувалось для вчинення шахрайських лій; відмова від дачі показань [41, с. 91].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було виявлено такі способи приховування кримінальних правопорушень, пов’язаних із використанням е-банкінгу:

1) ліквідацію устаткування, що застосовувалося для скоєння протиправних дій – 39 %;

2) надання завідомо неправдивих показів під час здійснення процесуальних дій (так само і неправдиве алібі) – 45 %;

3) відмову від надання показів – 58 %;

4) маскування шпигунського програмного або технічного забезпечення під його законні аналоги – 46 %;

5) застосовування зміни ідентифікатора місця знаходження обладнання, за допомогою якого були скоєні протиправні дії при застосовуванні е-банкінгу – 78 %.

Так, 11.01.2021, приблизно о 20 год. 00 хв., гр. В., маючи злочинний умисел на незаконне втручання в роботу автоматизованої системи, перебуваючи за місцем свого проживання, з метою отримання доступу до платіжних карток потерпілої гр. Ю., яка 09.01.2021 передала для проведення обслуговування з ремонту працівникам магазину «Device», що знаходиться в ТЦ «Екватор», власний мобільний телефон, в якому знаходилась сім-карта оператора стільникового зв'язку ПрАТ «Київстар», а також було встановлене програмне забезпечення у вигляді застосунків «Приват24» (мобільний додаток е-банкінгу АТ КБ «Приватбанк»), «Дія» (мобільний застосунок, розроблений Міністерством цифрової трансформації України), в яких використовувалися її облікові записи, отримавши наступного дня, тобто 10.01.2021, вказаний мобільний телефон від працівника магазину «Device» із зобов'язанням провести його ремонт, використовуючи власний мобільний телефон, здійснив несанкціоноване втручання до облікового запису потерпілої в е-банкінгу «Приват24», підробивши відомості про засоби верифікації гр. Ю. за допомогою сім-картки оператора стільникового зв'язку ПрАТ «Київстар» [181].

Крім того, слід наголосити на чинниках, котрі впливають на вибір способів вчинення протиправних дій, пов'язаних із використанням е-банкінгу, а саме: умови запровадженого воєнного стану; загальна обстановка,

що склалася у державі; ситуація у конкретному регіоні (області), особистісні якості потерпілої сторони, наявність певних злочинних вмінь і навичок у правопорушника та ін.

Підсумовуючи, зазначимо, що для розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, найбільш важливе значення з усіх складових криміналістичної характеристики буде мати спосіб їх учинення. Встановлено такі підготовчі заходи, як: 1) знаходження потрібної електронно-обчислювальної техніки (ноутбуків, комп'ютерів, планшетів); 2) підготовка підходящих обставин для реалізації протиправних дій та ін.; 3) виготовлення шпигунських технічних або програмних засобів для протиправного використання під час здійснення операцій е-банкінгу; 4) збут чи розповсюдження без необхідного дозволу мережею Інтернет відомостей, що мають значення під час здійснення операцій е-банкінгу. Визначено безпосередні способи вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, зокрема: 1) протиправні дії при застосовуванні е-банкінгу; 2) протиправні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 3) протиправні дії з відомостями, що знаходяться в пам'яті електронно-обчислювальної техніки; 4) поширення шпигунських програмних чи технічних засобів, а також їх збут із застосовуванням мережі Інтернет. З'ясовано також способи приховування зазначених кримінальних правопорушень, як-от: 1) ліквідація устаткування, що застосовувалося для скоєння протиправних дій; 2) надання завідомо неправдивих показів під час здійснення процесуальних дій (так само як і неправдиве алібі); 3) відмова від надання показів; 4) маскування шпигунського програмного або технічного забезпечення під його законні аналоги; 5) застосовування зміни ідентифікатора місця знаходження обладнання, за допомогою якого були скоєні протиправні дії при застосовуванні е-банкінгу.

1.3. Обстановка та слідова картина кримінальних правопорушень, пов'язаних із використанням е-банкінгу

Обстановка вчинення протиправного діяння наявна майже в кожній існуючій криміналістичній характеристиці. І це зрозуміло, адже місце, час, умови вчинення мають сталі кореляційні зв'язки як зі способом вчинення, так і з іншими елементами визначеної наукової категорії [116, с. 132].

У межах власного дослідження М. Куратченко зазначав: «…обстановка вчинення злочину – це широке поняття, що включає ряд елементів, які характеризують середовище, в якому вчинюється суспільно-небезпечне діяння. Поміж них обов'язково необхідно виділяти час, місце і умови вчинення злочину, що мають значення для його повного дослідження. …Місце вчинення злочину слід досліджувати з різних боків. Зокрема, з однієї сторони, як географічне поширення досліджуваного кримінально караного посягання, з іншої – конкретне місце його вчинення. …Воно містить великий об'єм відомостей щодо способу скоєння кримінального правопорушення, певних даних про особу злочинця» [97, с. 238]. У свою чергу, В. Шепітько формулює обстановку вчинення протиправних діянь як «…частину матеріального середовища, що містить, крім ділянки території, сукупність різних предметів, поведінку учасників події, психологічні взаємовідносини між ними» [129, с. 184].

А вже О. Сіренко зауважила, що «…до обстановки вчинення злочину найбільш доцільно включити місце і час вчинення злочину; об'єкт і предмет злочинного посягання; склад учасників; матеріальні елементи оточуючого середовища; зв'язки, що існують між вказаними елементами і іншими елементами криміналістичної характеристики» [176, с. 224]. Така думка авторки, на наш погляд, є дещо помилковою, позаяк, крім правильно зазначених елементів, таких як місце й час, дослідниця визначила складові, загалом не характерні для обстановки вчинення протиправних діянь, зокрема

матеріальні елементи оточуючого середовища та склад учасників.

Зі свого боку, Є. Буждиганчук визначила обстановку «…через сукупність об'єктивних і суб'єктивних факторів й умов матеріальної обстановки, соціально-економічних та соціально-психологічних чинників, просторово-часових характеристик місця і часу, а також особливостей впливу непрямих учасників події на процес підготовки, учинення й приховування правопорушення» [21, с. 123]. У розрізі визначеного вважаємо досить слушною позицію В. Локтіонової, яка значення об'єктивної сторони злочину формулює такими притаманними ознаками та властивостями: «…є обов'язковою для будь-якого складу злочину, її відсутність виключає злочинність і караність вчиненого. Також слід враховувати, що наявність чи відсутність однієї або декількох ознак об'єктивної сторони може істотно вплинути на кваліфікацію діяння. Наприклад, у разі, якщо з незалежних від винного причин не настає наслідок при вчиненні складу з матеріальною конструкцією об'єктивної сторони, вчинене кваліфікується як незакінчений злочин; – є головним критерієм розмежування суміжних складів злочинів. При цьому до уваги беруться як обов'язкові, так і факультативні ознаки об'єктивної сторони складу злочину. Головним моментом при цьому є характеристика діяння і способу вчинення злочинного діяння. Наприклад, дві форми вчинення діяння, передбаченого ст. 146 КК – викрадення людини або незаконне позбавлення волі, – відрізняються одна від одної способом вчинення. При викраденні людини потерпілий захоплюється і переміщається в інше місце, у той час як незаконне позбавлення волі пов'язане з утриманням особи в місці звичайного для потерпілого перебування. Водночас, проводячи розмежування різних злочинів, слід враховувати й інші ознаки об'єктивної сторони: характер наслідків, місце, час, знаряддя вчинення посягання. Так, одна з відмінностей бандитизму (ст. 257 КК) від створення злочинної організації (ст. 255 КК) виявляється у знарядді вчинення злочину. Обов'язковою ознакою об'єктивної сторони бандитизму є наявність зброї, тоді як у злочині, передбаченому ст. 255 КК, ця ознака вважається

факультативною; – дозволяє розмежувати злочинне діяння від незлочинного. У цьому разі необхідно брати до уваги всю сукупність обставин справи, що характеризують зовнішню сторону протиправного діяння: спосіб посягання, розмір заподіяної шкоди, місце та обстановку його вчинення. Наприклад, кримінально каране хуліганство (ст. 296 КК) відрізняється від аналогічного адміністративного делікту – дрібного хуліганства – за ступенем порушення громадського порядку. Кримінальний делікт, на відміну від адміністративного, пов'язаний не просто з порушенням громадського порядку, а виражається у грубому порушенні правил поведінки в громадських місцях. Крім того, кримінально каране хуліганство має бути поєднане із застосуванням насильства чи погрозою його застосування, або зі знищенням чи пошкодженням майна. У дрібному хуліганстві ця ознака відсутня; істотно впливає на ступінь суспільної небезпеки злочину і, як наслідок, на вид і розмір (строк) покарання. Наприклад, настання в результаті вчинення злочину тяжких наслідків значно підвищує ступінь його шкідливості. У багатьох випадках на розмір небезпеки злочину впливає спосіб його вчинення» [108, с. 251–252].

З іншого боку, О. Астахова зауважила, що «…для фахівця-криміналіста зазначена наукова категорія є важливим джерелом, яке важко відтворити з метою отримання об'єктивної первинної інформації про подію злочину та особу злочинця, яка його вчинила. Для кримінолога – вона є вихідним матеріалом для розробки і запровадження профілактичних заходів та запобігання злочинам. Для особи, яка застосовує закон, представляє інтерес: з позиції загальної теорії складу злочину; в індивідуалізації суспільно небезпечного діяння; в розмежуванні злочину від іншого аналогічного правопорушення; в розмежуванні суміжних злочинів; для з'ясування умов кримінальної відповідальності; з позиції необхідності характеризувати самі (конкретні) зовнішні ознаки суспільно небезпечного діяння; з позиції характеристики умов вчинення суспільно небезпечного діяння (тобто в яких умовах відбувається суспільно небезпечне діяння)» [3, с. 90]. Досить цікавим

є визначення В. Динту, яка сформулювала обстановку вчинення кримінального правопорушення як «…систему відомостей, які відображають матеріальні, мікро-соціальні та морально-психологічні умови його підготовки, вчинення та приховування» [26, с. 8].

Інший дослідник, Б. Черняховський у межах вивчення обстановки вчинення шахрайства у сфері банківських електронних платежів та суміжних йому кримінальних правопорушень констатував, 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» [201, с. 59].

З огляду на вищенаведені позиції та думки науковців сформулюємо власне визначення обстановки вчинення протиправних діянь як комплексу об'єктивних та суб'єктивних чинників матеріального світу, а також просторово-часових ознак місця та часу, котрі впливають на підготовку, вчинення та приховування протиправного діяння.

Доречною вважаємо думку Л. Брича, який із приводу місць учинення протиправного діяння зауважував, що для окреслення ознак указаних місць необхідно відповісти на такі запитання: «…1) чи охоплюється поняттям «місце вчинення кримінального правопорушення» лише місце вчинення шахрайства – розташування ЕОТ за місцем проживання (роботи) злочинця чи за місцем проживання потерпілої особи; 2) чи поширюється поняття місце вчинення шахрайства на місцезнаходження інших ознак складу кримінального правопорушення; 3) як відрізнити випадки, коли певні просторові характеристики є місцем вчинення суспільно небезпечного діяння й, відповідно, самостійною ознакою шахрайства – місцем його вчинення, від випадків, коли ті чи інші просторові характеристики стосуються інших ознак складу шахрайства» [20, с. 269].

На основі узагальнення наукових розробок учених нами було охарактеризовано об'єктивні умови, у яких вчинюються кримінальні

правопорушення, пов’язані з використанням е-банкінгу. Також було з’ясовано, що обстановка є найбільш дискусійною складовою криміналістичної характеристики кримінальних правопорушень, оскільки, по-перше, майже весь процес протиправної діяльності відбувається у віртуальному просторі; по-друге, вчинення протиправних дій може відбуватися як у різних регіонах держави, так і за її межами.

Аналіз судово-слідчої практики [Додаток А] дозволив дійти висновку, що 74 % кримінальних правопорушень, пов’язаних із використанням е-банкінгу, не мають конкретно визначеного місця події. Крім того, до обстановки віднесено такі складові:

1) час, протягом якого здійснювалися злочинні дії;

2) час, коли настали наслідки від протиправних дій;

3) місце реалізації злочинних дій (віртуальне середовище, в якому вчиняються дії, і місця, де знаходяться точки доступу – IP-адреси).

Дослідник С. Самойлов визначив місцями вчинення протиправних діянь: «…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» [168, с. 8].

На основі вивчення матеріалів кримінальних справ та проваджень [Додаток А] нами було визначено та охарактеризовано місця учинення злочинних дій, пов’язаних із використанням е-банкінгу:

– місця розміщення ЕОТ, що була застосована для вчинення протиправних дій (смартфон, комп’ютер, ноутбук, планшет) – 74 %;

– місця розташування банкоматів, банків, а також інших підприємств фінансової сфери – 16 %;

– місце розташування потерпілої особи, на яку були спрямовані

протиправні дії – 9 %.

Наприклад, гр. І. з 20.04.2023 вирішила незаконно заволодіти шляхом обману грошовими коштами користувачів соціальної мережі «Facebook» під приводом збору грошових коштів на позашляховик та тепловізор для механізованої роти, де проходить військову службу її чоловік. З цією метою, маючи вільний доступ до соціальної сторінки «Facebook» свого чоловіка та його особистого банківського рахунку, розмістила відповідне оголошення та вказала номер картки чоловіка, відкритий в АТ КБ «Приватбанк». У подальшому, після надходження грошових коштів від користувачів соціальної мережі «Facebook» на вказаний в оголошенні рахунок, правопорушниця, використовуючи відкритий на ім’я чоловіка е-банкінг «Приват24», забезпечувала переведення цих коштів із банківської картки (рахунку) свого чоловіка на власну банківську карту (рахунок), відкриту в АТ «Ощадбанк». У подальшому, отримавши повний доступ до незаконно здобутих грошових коштів, гр. І., діючи з корисливих мотивів, переводила частину грошових коштів із власної банківської картки АТ «Ощадбанк» на придбані нею в мережі Інтернет онлайн-карти, відкриті на інших осіб, котрі за допомогою блокчейн-системи використовувала на криптовалютній біржі «Binance», частину коштів під вигаданими приводами перераховувала на банківські карти (рахунки) своїх родичів, які, на вимогу правопорушниці, віддавали їй готівкові кошти на еквівалентну перерахованій суму, частину коштів витрачала на власні потреби в закладах та об’єктах торгівлі [182]. Як бачимо, для вчинення протиправних діянь із використанням е-банкінгу правопорушниця використовувала власну ЕОТ.

Як вказує група авторів (Н. Павлова, В. Рец), «…з’ясування початку і закінчення злочинних дій та їх тривалості у часі має велике значення для визначення часу безпосереднього закінчення шахрайства» [139, с. 142]. Водночас вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, може характеризуватися відносно тривалим часовим проміжком. Оскільки правопорушнику потрібен час як для

підготовчого етапу (підготовка ЕОТ, необхідного програмного забезпечення), так і для дій із приховування.

Окрема група дослідників (О. Дубовий, М. Салтевський, П. Тимошенко) влучно вказує на те, що, безумовно, «…частіше від комп'ютерних злочинів страждають більш розвинуті у технічному відношенні країни, однак й інші країни з початком процесу комп'ютеризації стають родючим ґрунтом для вчинення таких злочинів. Зокрема, глобальна комп'ютерна мережа Інтернет надає можливість увійти до будь-якої американської відомчої комп'ютерної системи, у тому числі і військової. До того ж, це можливо зробити майже з будь-якої точки світу. У порівнянні з США, національна безпека України поки що залежить від комп'ютерних мереж значно менше. На сьогодні ми стикаємось з комп'ютерними злочинами, в основному у фінансово-кредитній сфері. Але у недалекому майбутньому такі злочини можуть привести до глобальних катастроф – екологічних, транспортних тощо. Введення сучасної системи управління повітряним рухом, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання комп'ютерів у діяльності правоохоронних органів та керуванні військами значно розширили сферу діяльності для хакерів» [82, с. 364–365].

Інша група науковців (П. Біленчук, Д. Біленчук, О. Котляревськиий) зауважила: «…характерні риси комп'ютерної злочинності: як правило, міжнародний характер злочину (виходить за рамки кордону однієї держави); труднощі у визначені «місцезнаходження» злочину; слабкі зв'язки між ланками в системі доказів; неможливість спостерігати і фіксувати докази візуально; широке використання злочинцями засобів шифрування інформації. Громадськість все більше цікавиться цими питаннями, оскільки кожний власник або користувач комп'ютера – це потенційний потерпілий, якого можуть очікувати тяжкі наслідки в разі вчинення злочину, особливо у комерційному та промисловому секторі, де можливі великі фінансові втрати. Комп'ютерні злочинці за допомогою міжнародних комп'ютерних мереж –

типу Інтернет – широко розповсюджують свій кримінальний досвід, не звертаючи увагу на національні кордони, що вимагає відповідних кроків кооперації від поліцейських установ, протидіючих цим злочинам. Все це вимагає оперативного обміну інформацією про комп'ютерні злочини» [82, с. 365].

Стосовно вчинення шахрайства в Україні окремі дослідники вказують: «…якщо в країні мінімальна заробітна плата є низькою, тоді населення країни більше схильне до шахрайських операцій, ніж у суспільстві, в якому вища заробітна плата; в країні, в якій велика кількість населення має дохід нижче валового доходу, схильність до здійснення шахрайських операцій зростає; коли в країні йде поширення корупційної складової, то схильність до здійснення шахрайських операцій буде збільшуватися; коли суспільство не має право вибору на бажану роботу, виробництво товарів, різних витрат та інвестицій, тоді в населення виникає схильність до здійснення шахрайства більше, ніж в суспільстві, яке має вільні економічні права; країна, в якій економічний розвиток не на високому рівні, купівельна спроможність населення низька, то можливе виникнення шахрайських операцій; висока схильність до виникнення шахрайства буде в регіонах, в яких буде збільшуватися рівень цін на товари та послуги, які купує населення для невиробничого споживання, а купівельна спроможність населення буде залишатися на низькому рівні. Вибір цих факторів обумовлений тим, що різні макроекономічні дії в країні спричиняють формування в населення схильності до здійснення шахрайства» [59, с. 106].

Щодо специфіки слідів досліджуваної категорії кримінальних правопорушень, зокрема, А. Рейнгольд зазначав таке: «…шахрайство в інтернет-комерції характеризується специфікою слідів, що можуть залишатися на таких носіях: пам'яті телефону – 78 %, сім-картці – 48 %, комп'ютері – 81 %, сервері мобільного оператора – 18 % або інтернет-провайдера – 17 %, флешці чи зовнішньому вінчестері – 38 %, пам'яті електронного журналу банкомату (терміналу) – 67%, історії платіжних

переказів через банківську систему – 78 %, квитанціях і роздруківках про електронні банківські платежі – 51 %, банківських картках – 37 %, пам'яті системи відеоспостереження (зал інтернет-кафе, фойє банку, місце біля банкомату) – 31 %, слідах папілярних ліній на засобах комп'ютерної техніки, клавіатурі терміналу – 38 % та ін.» [155, с. 14].

Окрема група науковців (Б. Головкін, О. Денькович, В. Луцик, Д. Цехан) вказала на те, що, видається, «…саме з такими підходами пов'язано введення у науковий обіг поняття «електронного речового доказу», яке вчені використовують без належного обґрунтування. Так, під «електронним речовим доказом» розуміють технічний пристрій, що завдяки своїм індивідуальним чи системним (тим, які проявляються тільки при одночасному використанні з іншими об'єктами) властивостям слугував знаряддям злочину або зберіг на собі сліди злочину, а також може слугувати засобом для виявлення злочину чи встановлення істини у кримінальній справі. Впровадження означеного терміна обґрунтовується наявністю особливостей, що відрізняють його від традиційних речових доказів, – "віртуальна природа закріплення інформації на них"» [60, с. 130].

Зі свого боку, Т. Коршикова стосовно слідів, що характеризують місце події, вказувала на наявність таких, як: «…електронно-обчислювальна техніка (комп'ютери, їх системні блоки, ноутбуки); монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, джойстики та інше, комунікаційні прилади комп'ютерів і обчислювальних мереж; жорсткі диски, оптичні диски, флешпам'ять; засоби зв'язку (у разі їх використання під час вчинення шахрайства) (на стільникових апаратах, засобах телекомунікації, спеціальних електронних картках, електронних ключах доступу до персонального комп'ютера; пристроях упізнання користувача); електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них; сліди пальців рук і мікрочастинки або мікрооб'єкти (наприклад, частки волосся), які можуть залишатися на вказаних вище предметах; сліди, що залишаються на «робочому» місці

злочинця, (наприклад, які-небудь рукописні записи – списки паролів, коди, чернетки тощо)» [75, с. 66–67].

У межах досліджуваної категорії кримінальних правопорушень більшість протиправних дій відображається у віртуальних, цифрових або комп'ютерних слідах. Вказані електронні сліди здебільшого вилучаються з таких місць: профілів соціальних мереж та онлайн-магазинів, кеш-пам'яті акаунтів і веббраузерів, флеш-носіїв, месенджерів («Телеграм», «Фейсбук», «Інстаграм», «Твіттер») для криптовалютних листувань, пам'яті та кеш-пам'яті ЕОТ, бази інтернет-провайдерів. У випадках безпосередньої зустрічі зі злочинцем чи спілкування з ним у форматі відеоконференції потерпілий може вказати відомості про його зовнішність.

Слідова картина кримінальних правопорушень, пов'язаних із використанням е-банкінгу, охоплює 3 групи слідів: 1) матеріальні сліди, що містяться на різноманітних матеріальних носіях інформації (квитанції, банківські картки, сім-картки, паперові копії даних із ЕОТ, відбитки папілярних ліній на ЕОТ, клавіатурі банкомата); 2) ідеальні сліди, що становлять відомості у пам'яті потерпілих, підозрюваних та осіб, які були свідками незаконних операцій із використанням е-банкінгу; 3) віртуальні сліди (пам'ять ЕОТ, кеш-пам'ять серверів інтернет-провайдерів, пам'ять смартфонів, кеш-пам'ять електронного реєстру термінала чи банкомата тощо).

Підсумовуючи, зазначимо, що опрацювання обстановки вчинення кримінальних правопорушень із використанням е-банкінгу відіграє важливу роль як на початковому, так і подальших етапах розслідування. Підтримується позиція, що складовими елементами обстановки вчинення кримінального правопорушення є місце, час, а також характер та умови скоєння протиправного діяння.

1.4. Характеристика особи правопорушника та потерпілого

Особа правопорушника є особливим елементом криміналістичної характеристики з огляду на те, що під час вчинення будь-якого протиправного діяння вказана складова буде наявна в будь-якому випадку. Оскільки без діяльності конкретної особи не може бути вчинено жодного кримінального правопорушення.

В розрізі зазначеного підтримуємо позицію окремої групи дослідників (П. Біленчук, О. Дубовий, М. Салтевський, П. Тимошенко), які вказали, що криміналістика насамперед вивчає «професійні» звички правопорушників. Зокрема, автори наголосили, що такі звички «…проявляються, в основному, в певних способах і прийомах учинення злочинів, залишають на місці вчинення злочинів характерний «почерк» злочинця: результати кожної злочинної діяльності містять сліди людини, яка їх залишила. Виявлення на місці вчинення злочину речових доказів проливають світло як на відомості про деякі його особисті соціально-психологічні ознаки, так і на відомості про його злочинний досвід, професію, соціальні знання, стать, вік, особливості взаємодії з потерпілим. Криміналістично значимі дані про особу злочинця в даний час базуються на двох специфічних групах інформації. Перша група включає до себе дані про особу невідомого злочинця по залишених ним слідах як на місці події, в пам’яті свідків, так і за іншими джерелами з метою встановлення напрямку і прийомів його розшуку і затримання. Така інформація дає уяву про загальні ознаки певної групи осіб, серед яких може бути і злочинець. Такі відомості слід співставляти з наявними криміналістичними даними про особу, яка скоріше всього вчинює злочини розслідуємого типу. Друга група об’єднує інформацію, яка отримана за допомогою вивчення особи затриманого підозрюваного чи обвинувачуваного з метою вичерпної криміналістичної оцінки особи – суб’єкта злочину. З цією метою збираються відомості не тільки про ціннісні орієнтації, особливості

антисуспільних поглядів, але і про те, яка інформація найбільше характеризує особу суб'єкта злочину, його зв'язки, особливості поведінки до, під час і після вчинення злочину, може допомогти слідчому чи оперативному працівнику знайти зі злочинцем необхідний психологічний контакт, отримати правдиві свідчення, а також вибрати найбільш дієві способи профілактичного впливу на нього. Вважається, що ця інформація, з врахуванням відомостей про злочинців, які відображаються в інших елементах криміналістичної характеристики, може бути покладена в основу типізації злочинців. Формування банку типових моделей різних категорій злочинців, вивчення загальних рис цих людей дозволяє оптимізувати процес виявлення кола осіб, серед яких потрібно вести пошук злочинця типу» [82, с. 367–368].

Стосовно визначення поняття особи правопорушника для початку звернемося до формулювання, наданого А. Зелінським, а саме: «…сукупність соціально-демографічних, психологічних та моральних характеристик, які в тій чи іншій мірі типово притаманні людям, винним у злочинній діяльності певного типу» [53, с. 57]. Згідно з ч. 1 ст. 18 КК України суб'єктом злочину є фізична осудна особа, яка вчинила злочин у віці, з якого відповідно до цього кодексу може наставати кримінальна відповідальність [87]. З огляду на зазначене вважаємо за доцільне привести твердження групи авторів, які зауважили, що «…це визначення характеризує поняття загального суб'єкта, тобто містить у собі таку сукупність ознак, що є обов'язковою для особи, яка вчинила будь-який злочин. Отже, кримінальній відповідальності і покаранню може підлягати особа тільки при наявності трьох ознак: а) фізична, б) осудна, в) яка досягла певного віку» [88, с. 55].

У свою чергу, В. Бедь наводив таку тезу: «…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» [6, с. 151].

Також варто навести позицію В. Логінової, яка надала таку класифікацію груп ознак, що характеризують особу правопорушника: «…1) біографічні дані: прізвище, ім'я, по-батькові; дата та місце народження; національність, громадянство, місце проживання, освіта, спеціальність, стаж роботи; сімейний стан, склад родини; попередня судимість; 2) дані про матеріальний стан: загальний дохід і житлові умови сім'ї (для неповнолітніх) тощо; відомості про стан здоров'я й психологічні особливості: загальний стан здоров'я; фізичні вади; наявність стійкої хвороби, групи інвалідності; дані про характер, темперамент, вольові та емоційні властивості; 3) суспільно-виробнича характеристика: термін роботи або навчання в певному місці; ставлення до такої діяльності, товаришів по роботі (навчанню); участь у громадському житті; наявність дисциплінарних або громадських стягнень та заохочень; 4) суспільно-політична характеристика: членство у політичній партії, молодіжній, громадській організації; участь у виборчих кампаніях, збройних конфліктах; наявність нагород та почесних звань; 5) суспільно-побутова характеристика: взаємовідносини в родині; спосіб життя й коло знайомих; вживання алкоголю; відносини із сусідами; участь у громадській роботі за місцем проживання; наявність адміністративних або громадських стягнень; 6) ставлення до скоєного та поведінка в ході слідства; ціннісні орієнтири особистості; мотиви та мета скоєння злочину; наявність сп'яніння при вчиненні злочину тощо» [107, с. 116–118].

Зі свого боку, О. Лужецька акцентувала увагу на тому, що особа злочинця являє собою «…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» [109, с. 200]. Інший автор, В. Тіщенко навів таку систему ознак та властивостей особи правопорушника: «…1) біологічні, що містять статеві, вікові, анатомічні, фізіологічні й інші ознаки; 2) психічні, що свідчать про інтелект, емоційну та вольову сфери індивіда; 3) соціальні, що характеризують його суспільний статус, професійну належність, родинний стан, місце проживання, рід занять, взаємини з іншими людьми тощо» [187, с. 105].

У розрізі зазначеного наведемо твердження І. Даньшина стосовно того, що «…особа злочинця включає низку елементів, тобто певну кількість різних ознак, властивостей, рис, особливостей…: соціально-демографічні ознаки (відомості про стать, вік, рівень освіти, рід занять, стаж роботи, сімейний стан, місце проживання, інші дані про соціальний статус особи). Соціально-демографічні ознаки дають істотну інформацію про особу злочинців, що може бути використана як із науковою, так і прикладною метою, зокрема під час розробки та реалізації заходів запобігання злочинам; особистісно-рольові властивості (соціальні позиції, рольові особливості тощо); соціально-психологічні якості (особливості особи, які сформувалися на базі її психічних станів і процесів у ході власного соціального досвіду; спрямованість особистості, мотиваційна сфера, потреби, установки, інтереси тощо); риси правової й моральної свідомості; кримінально-правові ознаки (спрямованість злочинної поведінки суб’єкта на конкретні суспільні відносини, узяті під охорону законом; ступінь і характер суспільної небезпечності вчиненого злочину; способи, обрані для досягнення злочинної мети; мотив, яким керувався суб’єкт злочину; ставлення винного до вчиненого)» [91, с. 37–38]. Окрема група науковців (І. Пиріг, В. Самсонова) вказує, що «…для повної характеристики особи злочинця необхідно мати такі дані: фізико-біологічні властивості особи (стать, вік, зріст, статура, фізичні дані тощо); соціально-демографічні (національність, освіта, сімейний стан тощо); морально-

психологічні (світогляд, переконання, риси характеру, звички, емоції, темперамент тощо); соціально-побутові (місце проживання, роботи, навчання, суспільні відносини при виконанні окремих видів діяльності); соціально-правові (злочинний досвід, наявність судимості, ставлення до вчиненого тощо)» [170, с. 32]. Тобто більшість дослідників, опрацьовуючи визначення особи правопорушника, виокремлює як її загальні ознаки та властивості, так і особисті.

З приводу осіб, які вчиняють кримінальні правопорушення з використанням е-банкінгу, підтримуємо І. Коваленка, який вказав, 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» [66, с. 84].

Наостанок вважаємо доречним навести позицію окремої групи дослідників (П. Біленчука, О. Дубового, М. Салтевського, П. Тимошенка), які дійшли такого висновку: «…характеризуючи особу комп'ютерного злочинця, необхідно відмітити основну ознаку, а саме: в електронну злочинність втягнуто широке коло осіб, від висококваліфікованих фахівців до дилетантів. Правопорушники приходять з усіх сфер життя і мають різні рівні освіти (навчання та виховання). З метою глибшого вивчення цієї проблеми необхідно чітко знати: хто ж вони, комп'ютерні злочинці? Вітчизняні та зарубіжні дослідження дають змогу намалювати портрет типового комп'ютерного злодія, тобто відповідний профіль (портрет) даного соціального типу» [82, с. 368].

Отже, вбачаємо за необхідне виокремити групи криміналістично значущих ознак особи правопорушника, який вчиняє кримінальні правопорушення з використанням е-банкінгу, як-от:

а) фізичні;

б) соціально-демографічні;

в) інтелектуальні;

г) моральні.

Стосовно досліджуваної групи правопорушників вважаємо слушною думку О. Севідова, який, опрацювавши низку наукових публікацій, виокремив такі групи кіберзлочинців, як кардери, фішери, спамери, кіберкруки, фрікери, кіберсквотери. Автор аргументував такий поділ схильністю окремих категорій осіб вчиняти протиправні діяння у відповідний спосіб. Зокрема, для спамерів характерною є розсилка спам-листів, для фішерів – посилань із вірусним програмним забезпеченням тощо [171].

Доречним із огляду на зазначене вважаємо твердження, надане А. Боровиком та І. Копотуном: «…багато з цих ознак трапляється при вчиненні кіберзлочинів, а тому при їх кваліфікації слід приділити увагу відсутності їх всіх. Зокрема, найчастіше виникає питання про відсутність двостороннього суб'єктивного зв'язку між особами, з участю яких вчиняється злочин, – при вчиненні кіберзлочину його учасники іноді навіть не бачили один одного ніколи і не спілкувалися в реальному житті. А тому слід установити факт їх спілкування в кіберпросторі про вчинення злочину, який або передував йому (група за попередньою змовою, організована група, злочинна організація) або відбувався під час його вчинення (група осіб). Якщо такий факт відсутній, то діяння всіх осіб кваліфікуються за відсутності ознак співучасті» [19, с. 99]. Тобто необхідно встановити безпосередній факт спілкування правопорушників для встановлення їх співучасті та її форми (ОГ чи ЗО). Це можна зробити шляхом огляду ЕОТ кіберзлочинців, зняття інформації з телекомунікаційних та інших мереж, встановлення візуального спостереження за особою тощо.

Зі свого боку, А. Рейнгольд наводить класифікацію осіб, які вчиняють шахрайство в інтернет-комерції, а саме: «…фізична особа, що пропонувала товар, у тому числі не існуючий; юридична особа, дані про яку розміщені в

Єдиному державному реєстрі юридичних осіб, що пропонувала товар, у тому числі не існуючий; банківський працівник; посередники – провайдери, або оператори в системі мережі Інтернет та інші суб'єкти, що надають різноманітні види послуг; покупець» [156, с. 69].

А вже І. Коваленко робить висновок, що шахрайство у сфері використання банківських електронних платежів «…в основному вчиняють особи чоловічої статі у віці 25-35 років, які мають вищу освіту, неодружені та працюють у сфері підприємницької діяльності та сфері комп'ютерних технологій» [66, с. 90].

У свою чергу, Г. Римарчук та В. Мельник вказують на те, що «…одним із основних елементів кіберзлочинів є неправильне використання програмного забезпечення та засобів інтернет-користування. Злочинці у своєму арсеналі мають безліч способів втручання в особистий простір індивіда, такі як електронна пошта, персональні веб-сторінки тощо. В даному випадку злочинці використовують паролі доступу та засоби дистанційного доступу. Засоби дистанційного доступу були створені з метою виправлення неполадок системи, однак їх можна використовувати і як засіб незаконного посягання на інформацію. Кіберзлочинці можуть використовувати мікрофони та камери на комп'ютері користувача для спостереження за діями останнього. Ще однією ознакою кіберзлочинів є персоналізація, видача себе за іншу особу, що дозволяє злочинцям проникнути та заволодіти інформацією. Вони ховаються за рекламними акціями, подарунковими сертифікатами, безкоштовними пропозиціями. Вони також знають, як видати себе за відому організацію чи установу, пропозиції чи запитання від якої виглядали б абсолютно законно та не викликали підозри. Так, наприклад, одним із способів доступу до персональних даних є прохання підтвердити свій пароль в онлайн банкінгу чи номер рахунку під виглядом виникнення проблеми з онлайн рахунком клієнта» [158, с. 56]. Зі свого боку, К. Заяць наголошував на тому, 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» [48, с. 98]. Як бачимо, автори акцентували увагу на тому, що правопорушники (кіберзлочинці, шахраї) є своєрідною елітою в злочинному світі, яка має свої особливості як щодо морально-ділових якостей, так і стосовно підготовки матеріального забезпечення для вчинення протиправних діянь.

На основі вивчення матеріалів кримінальних справ та проваджень [Додаток А] було встановлено та узагальнено криміналістично значущі типологічні ознаки особи правопорушника.

Зокрема, було визначено, що досліджувані протиправні діяння переважно скоюють чоловіки (81 %). Щодо вікових особливостей встановлено, що у 9 % випадків кримінальні правопорушення здійснюються особами віком від 16 до 20 років, у 34 % випадків – 20–30 років, у 31 % випадків – 30–40 років, у 20 % випадків – 40–50 років, у 6 % випадків – 50 років і старше.

Загалом більшість злочинців мають базову вищу (38 %) і повну вищу (42 %) освіту. Базову загальну середню освіту мають 3 % злочинців, повну загальну середню освіту – 5 %, професійно-технічну освіту – 12 %. Якщо злочинна діяльність здійснюється у складі ОЗГ, то повну загальну середню освіту мають переважно особи, які виконували другорядні ролі.

Здебільшого злочинці не є місцевими мешканцями (81 %).

Наведені відомості допомагають слідчому скласти найбільш вірогідний «портрет» особи злочинця, що дозволяє:

а) вчасно висувати слідчі версії щодо злочинної події;

б) окреслити чи звузити коло підозрюваних осіб;

в) організувати затримання злочинців «за гарячими слідами»;

г) вилучити знаряддя злочину (смартфони, комп’ютери, ноутбуки,

планшети, флеш-носії);

д) спрогнозувати тактику поведінки злочинця під час проведення СРД та інших процесуальних заходів;

е) вирішити низку інших завдань кримінального провадження.

Крім того, сформований типовий «портрет» особи злочинця відіграє важливу розшукову роль під час реалізації НСРД та пошукових заходів.

Також було встановлено, що властивою характеристикою злочинця є особливий вид ознак – інтелектуальні. Адже вказані особи (зокрема спеціалісти з комп'ютерного програмування, фахівці з використання ЕОТ, хакери, фішери, фрікери, спамери, кіберсквотери) повинні володіти достатнім рівнем інтелекту для реалізації своїх професійних функцій.

Отже, на основі вивчення матеріалів кримінальних справ та проваджень сформовано ймовірний «портрет» особи злочинця. З'ясовано, що особам, які вчиняють кримінальні правопорушення, пов'язані з використанням е-банкінгу, притаманні високий рівень інтелекту, винахідливість та комунікабельність. Властивою характеристикою особи злочинця (хакери, фішери, фрікери, спамери, кіберсквотери, спеціалісти з програмного забезпечення та використання ЕОТ) є особливий вид ознак – інтелектуальні. Ці особи мають спеціальні знання й навички у сфері електронного бізнесу, е-комерції, інтернет-торгівлі, здійснення банківських операцій, використання цифрових технологій, комп'ютерного програмування та ін. Здебільшого це чоловіки віком 20–40 років, які мають базову або повну вищу освіту.

Щодо значення особи потерпілого ми підтримуємо позицію О. Кравченка, який відмітив, що «…шахрайство в усіх випадках є результатом трьох складників: конкретної криміногенної ситуації, поведінки злочинця й потерпілого. Саме в цьому «трикутнику» міститься вузловий механізм здійснення шахрайського акту, оскільки, реагуючи на криміногенну ситуацію, яка склалась, обидві сторони діють згідно з особливостями своїх інтересів і поглядів, які нерідко в них співпадають» [79, с. 9].

Визначення терміна «потерпілий» надано законодавцем у ч. 1 ст. 49 КПК України, а саме: «Потерпілим визнається особа, якій злочином заподіяно моральну, фізичну або майнову шкоду» [89]. У свою чергу, М. Сенаторов наголошував на тому, що «…завдяки дослідженню теорії кримінального права, положень кримінального закону та практики його застосування зробив висновок, що потерпілий від злочину та обставини, пов'язані з ним, мають значення для встановлення соціальної сутності злочину, з'ясування характеру та ступеня його суспільної небезпечності, криміналізації та декриміналізації діянь, диференціації кримінальної відповідальності. Чітка вказівка на потерпілого та обставини, пов'язані з ним, дозволяють відмежувати один злочин від іншого; виступають ознаками складу переважної частини злочинів; сприяють конкретизації інших ознак складу; враховуються при кваліфікації злочинів та призначенні покарання, а також при вирішенні питань чинності закону про кримінальну відповідальність у просторі, звільнення від кримінальної відповідальності та відбування покарання» [173, с. 3].

Вважаємо правильним твердження О. Мусієнка, який зауважував, що розділення зв'язку між шахраєм та потерпілим залежить від наявності певних відносин між ними. Крім того, дослідник акцентував увагу, що за обставинами утворення зв'язок буває такий, що: «…1) розвинувся в результаті певних взаємин, які існували між злочинцем і його жертвою до вчинення кримінального правопорушення; 2) виник у результаті гостроконфліктної ситуації безпосередньо до або в момент вчинення кримінального правопорушення; 3) виник за відсутності якихось конфліктних взаємин між жертвою і злочинцем до вчинення кримінального правопорушення. Взаємини між майбутнім злочинцем і майбутнім потерпілим за своїм характером можуть бути різними: від хороших (близьких, інтимних, дружніх, приятельських) або таких, що мають байдужний, нейтральний характер, до неприязних, відверто ворожих» [127, с. 83–85].

Найбільш слушним вважаємо формулювання цієї наукової категорії, надане М. Сенаторовим, як-от: «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» [174, с. 60]. У межах криміналістичних досліджень вважаємо найбільш оптимальною позицію, що її озвучив А. Шеремет, а саме: «…дані про потерпілого займають важливе місце в криміналістичній характеристиці, особливо злочинів проти життя, здоров'я та гідності особистості. Це пояснюється двома обставинами: певною вибірковістю в діях злочинця, яка показує взаємозв'язок між особливостями особистості його і потерпілого; наявністю і характером зв'язків і стосунків між потерпілим і злочинцем, що впливають на мету, мотив, місце, час, способи скоєння та приховання злочину. Система ознак, що відносяться до особистості потерпілого, має складну структуру. Вона включає загальні демографічні відомості (стать, вік, місце проживання, навчання і роботи тощо), дані про спосіб життя, риси характеру, звички, зв'язки, стосунки (ворожі, дружні). Особливо важливе значення набувають дані про особу потерпілого у випадках, коли розслідування ведеться за справами про осіб, що пропали безвісті. Такі ситуації часто мають місце під час розслідування вбивств» [212, с. 345].

У свою чергу, Д. Птушкін вказував, що «…віктимність потерпілих проявляється й тоді, коли вони бажають при здійсненні правочинів заощадити кошти на майбутній угоді та ухилитись від сплати податків. Вивчення кримінальних проваджень, а також результати проведеного опитування показали, що потерпілими від шахрайства щодо об'єктів нерухомого майна громадян у 41 % випадках стають соціально незахищені верстви населення. Здебільшого шахраї посягають на нерухоме майно інвалідів із фізичними вадами (прикутих до ліжка); осіб похилого віку; осіб із вадами слуху та зору; осіб, в яких спостерігається розлад психіки, або неосудних

осіб; дітей-сиріт. Звісно, більшість вказаних осіб самостійно не можуть приймати рішення щодо здійснення угод із нерухомим майном, яке їм належить. Як ми раніше вже зазначали, для цього потрібний дозвіл певних суб'єктів (органів опіки та піклування та ін.). Між тим, шахраї вдаються до незаконного заволодіння нерухомим майном вказаних осіб через змову з такими суб'єктами або шляхом інших обманних дій» [150, с. 98].

А вже С. Головкін зауважував, що «…віктимність поведінки потерпілих виражена не лише у довірливості до інших людей чи у наявності негативних соціальних характеристик. Іноді самі власники майна створюють всі підстави для вчинення стосовно них шахрайства, наприклад, купують певне майно за значно заниженими цінами, не звертають уваги на інформацію про власника повідомлення (наявність установчих даних, телефону), користуються під час купівлі підозрілими сайтами і т. ін.» [24, с. 12]. Зі свого боку, С. Чучко відмічає, що потерпілими, які зазнали шкоди від шахрайських дій, «…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» [205, с. 92]. Як бачимо, дослідники визначають потерпілих з огляду на їхнє матеріальне становище, а також відносини з правопорушником.

Досить слушним вважаємо твердження К. Попова, який зауважував, що «…особистість жертви шахрайства становить інтерес з точки зору її віктимного потенціалу стосовно вказаного протиправного діяння, в її соціально-психологічному дослідженні, окрім вже названих, можна визначити певні додаткові орієнтири. ...Тому необачність потрібно розглядати не лише як сутнісну (сталу) властивість особистості, але і як одну з ознак поведінки у конкретній ситуації, яка залежить, з одного боку, від соціального досвіду особи, її поінформованості, звичок, інших особистісних властивостей, а з іншого – від впливу елементів зовнішнього середовища, у якому потенційна жертва опиняється у конкретний момент часу» [142, с. 164–165].

Також цікавою є думка Н. Павлової, яка вказувала, що «…легковір'я, довірливість потерпілих має свій прояв і у випадках, коли для здійснення правочинів з нерухомістю вони звертаються за допомогою до посередників, доручають їм розпоряджатися своїм майном та укладати угоди щодо житла. При цьому потерпілі не тільки не беруть участь у супроводженні угоди, а навіть не вдаються, яким чином відбувається процес відчуження житла. Проблема полягає у тому, що потерпілі не завжди усвідомлюють, що передають свої права людині, котра може скористатися можливістю, наданою самим потерпілим. Внаслідок цього особа втрачає своє житло, а шахрай, який виступає «посередником», отримує гроші від незаконного продажу житла. Зазначене свідчить про низький рівень правової культури громадян, що стає одним із факторів віктимності шахрайства, пов'язаного з нерухомістю» [135, с. 67].

Наостанок наведемо позицію І. Коваленка, який виокремив із-поміж віктимогенних груп потерпілих такі: «…а) особи, які піддалися впливу знайомих та родичів під час реалізації банківських електронних платежів; б) особи, які піддалися обману незнайомих осіб під час реалізації банківських електронних платежів; в) особи, які повідомили свої персональні дані працівникам банківської сфери; г) особи, які з огляду на негативні психічні

стани піддалися впливу незнайомих осіб під час реалізації банківських електронних платежів» [66, с. 93–94].

Отже, на основі вивчення матеріалів судово-слідчої практики [Додаток А] нами вирізнено віктимогенні групи осіб, стосовно яких було вчинено протиправні діяння, зокрема:

а) фізичні особи, які здійснювали купівлю-продаж товарів і послуг на онлайн-платформах та інтернет-аукціонах з використанням е-банкінгу;

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

в) їхні клієнти;

г) родичі клієнтів;

д) юридичні особи – при здійсненні матеріально-технічного постачання та інших заходів у випадках використання інтернет-банкінгу.

Висновки до розділу 1

З огляду на опрацювання проблематики, що характеризує поняття, сутність та структуру криміналістичної характеристики протиправного діяння, а також її складові, сформульовано такі висновки:

1. На основі аналізу праць науковців (як-от: А. Волобуєв, А. Іщенко, О. Пчеліна, М. Салтевський, В. Тіщенко, В. Шепітько) запропоновано систему окремої методики розслідування. Зокрема, з огляду на організаційно-тактичні особливості реалізації кримінальних проваджень, розпочатих за фактом учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, до неї включено такі складові: тактичні операції, взаємодію підрозділів правоохоронних органів, встановлення причин та умов, що сприяли вчиненню протиправного діяння.

2. Охарактеризовано наукові підходи стосовно сутності окремих наукових категорій, що визначають правовідносини у сфері використання

банківських електронних платежів, як-от: «електронна торгівля», «е-банкінг», «цифрова торгівля», «е-бізнес», «е-комерція» тощо, які відрізняються і мають різний зміст та наповнення.

3. Криміналістичну характеристику сформульовано як систему взаємопов'язаних відомостей про криміналістично значущі ознаки кримінального правопорушення, що поєднані відповідними кореляційними зв'язками та допомагають у розслідуванні завдяки побудові версій у результаті проведення окремих процесуальних дій та розшукових заходів.

4. Вирізнено такі складові криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як: спосіб і обстановка учинення кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого. Доведено, що зазначені елементи повинні бути максимально оптимізовані й спрямовані на вирішення практичних завдань кримінального провадження.

5. На основі вивчення матеріалів кримінальних проваджень та праць учених-криміналістів (як-от: О. Курман, Н. Павлова, О. Самойленко, С. Самойлов) з'ясовано, що повноструктурний склад способу вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, мав місце у 100 % діянь, адже майже в усіх випадках наявними є елементи підготовки та приховування кримінально караного діяння. Систематизовано підготовчі дії, а саме: 1) знаходження необхідної електронно-обчислювальної техніки (ноутбук, комп'ютер, планшет) із відповідним програмним забезпеченням; 2) виготовлення шпигунських технічних або програмних засобів для протиправного використання під час здійснення операцій е-банкінгу; 3) збут чи розповсюдження без необхідного дозволу у мережі Інтернет відомостей, що мають значення під час здійснення операцій е-банкінгу; 4) створення необхідної обстановки для реалізації протиправних дій та ін.

6. Охарактеризовано типові способи вчинення кримінальних правопорушень. Зосереджено увагу на способах приховування протиправних

діянь, а саме: знищення технічних пристроїв (устаткування), що застосовувалися для скоєння протиправних дій – у 72 % випадків; надання завідомо неправдивих показань або неправдивого алібі під час здійснення процесуальних дій – 45 %; відмова від надання показів – 58 %; маскування шпигунського програмного або технічного забезпечення під його законні аналоги – 46 %; застосовування зміни ідентифікатора місця знаходження обладнання, за допомогою якого скоєні протиправні дії при застосовуванні е-банкінгу – 78 %.

7. На основі узагальнення наукових розробок учених (О. Довженка, О. Мотляха, В. Сисолятіна, С. Чучка) охарактеризовано об'єктивні умови, в яких вчинюються кримінальні правопорушення, пов'язані з використанням е-банкінгу. З'ясовано, що обстановка є найбільш дискусійною складовою криміналістичної характеристики кримінальних правопорушень, оскільки, по-перше, майже весь процес протиправної діяльності відбувається у віртуальному просторі; по-друге, вчинення протиправних дій може відбуватися як у різних регіонах держави, так і за її межами. Доведено, що 74 % кримінальних правопорушень, пов'язаних із використанням е-банкінгу, не мають конкретно визначеного місця події.

8. Сформульовано авторське визначення обстановки вчинення протиправних діянь як комплексу об'єктивних і суб'єктивних чинників матеріального світу, а також просторово-часових ознак місця та часу, що впливають на підготовку, вчинення та приховування протиправного діяння. Визначено та охарактеризовано місця учинення злочинних дій, пов'язаних із використанням е-банкінгу: місця розміщення ЕОТ, що була застосована для вчинення протиправних дій (смартфон, комп'ютер, ноутбук, планшет) – 74 %; місця розташування банкоматів, банків, а також інших підприємств фінансової сфери – 16 %; місце розташування потерпілої особи, на яку були спрямовані протиправні дії – 9 %.

9. Розглянуто слідову картину та виокремлено кореляційні зв'язки між способами та слідами кримінальних правопорушень, пов'язаних із

використанням е-банкінгу, а також іншими елементами криміналістичної характеристики. Більшість протиправних дій відображається у віртуальних, цифрових або комп'ютерних слідах. Указані електронні сліди здебільшого вилучаються з таких місць: профілів соціальних мереж та онлайн-магазинів, кеш-пам'яті акаунтів і веббраузерів, флеш-носіїв, месенджерів («Телеграм», «Фейсбук», «Інстаграм», «Твіттер») для криптовалютних листувань, пам'яті та кеш-пам'яті ЕОТ, бази інтернет-провайдерів. У випадках безпосередньої зустрічі зі злочинцем чи спілкування з ним у форматі відеоконференції потерпілий може вказати відомості про його зовнішність. Виокремлено вузлові ділянки, де можуть бути зосереджені сліди злочинного діяння.

10. Встановлено криміналістично значущі типологічні ознаки особи злочинця, а також особливості віктимогенної поведінки особи потерпілого. Окреслено перелік ознак і властивостей, що характеризують особу злочинця, як-от: фізичні, соціально-демографічні, інтелектуальні та моральні. Встановлено та узагальнено криміналістично значущі типологічні ознаки особи злочинця. Визначено, що досліджувані протиправні діяння переважно скоюють чоловіки (81 %). Щодо вікових особливостей встановлено, що у 9 % випадків кримінальні правопорушення здійснюються особами віком від 16 до 20 років, у 34 % випадків – 20–30 років, у 31 % випадків – 30–40 років, у 20 % випадків – 40–50 років, у 6 % випадків – 50 років і старше. Загалом більшість злочинців мають базову вищу (38 %) і повну вищу (42 %) освіту. Базову загальну середню освіту мають 3 % злочинців, повну загальну середню освіту – 5 %, професійно-технічну освіту – 12 %. Якщо злочинна діяльність здійснюється у складі ОЗГ, то повну загальну середню освіту мають переважно особи, які виконували другорядні ролі. У переважній більшості випадків злочинці не є місцевими жителями (81 %).

11. Наведені відомості допомагають слідчому скласти найбільш вірогідний «портрет» особи злочинця, що дозволяє: а) вчасно висувати слідчі версії щодо злочинної події; б) окреслити чи звузити коло підозрюваних осіб; в) організувати затримання злочинців «за гарячими слідами»; г) вилучити

знаряддя злочину (смартфони, комп'ютери, ноутбуки, планшети, флеш-носії); д) спрогнозувати тактику поведінки злочинця під час проведення СРД та інших процесуальних заходів; е) вирішити низку інших завдань кримінального провадження. Сформовано типовий «портрет» особи злочинця, котрий відіграє важливу розшукову роль під час реалізації НСРД та пошукових заходів. Встановлено, що властивою характеристикою злочинця є особливий вид ознак – інтелектуальні. Адже вказані особи (зокрема спеціалісти з комп'ютерного програмування, фахівці з використання ЕОТ, хакери, фішери, фрікери, спамери, кіберсквотери) повинні мати достатній рівень інтелекту для реалізації своїх професійних функцій.

12. Надано характеристику особі потерпілого. Вирізнено віктимогенні групи осіб, стосовно яких було вчинено протиправні діяння, зокрема: а) фізичні особи, які здійснювали купівлю-продаж товарів і послуг на онлайн-платформах та інтернет-аукціонах із використанням е-банкінгу; б) працівники фінансових установ, підприємств та організацій різних форм власності; в) їхні клієнти; г) родичі клієнтів; д) юридичні особи – при здійсненні матеріально-технічного постачання та інших заходів у випадках використання інтернет-банкінгу. Зосереджено увагу на кореляційних зв'язках особи злочинця з потерпілим.

Основні результати розділу опубліковано у працях [112; 115; 116; 120].

РОЗДІЛ 2
ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ Е-БАНКІНГУ

2.1. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу

Початковий етап розслідування будь-якого кримінального правопорушення характеризується такими складовими: отриманням повідомлення про вчинене протиправне діяння, аналізом початкової інформації і, з огляду на її підтвердження, протягом доби внесенням відомостей до ЄРДР. Такий алгоритм заходів у більшості своїй зумовлює стислі строки реалізації початкових заходів для збору доказової бази, з-поміж яких найбільш важливим ми вбачаємо проведення огляду місця події. У кримінальних провадженнях, розпочатих за фактом вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, вказані заходи загалом обумовлюються відсутністю злочинця на місці події [118, с. 171].

У свою чергу, окрема група дослідників (М. Єфімов, І. Пиріг) зауважила, що «…систему планування можна розглядати як сукупність таких елементів: 1) аналіз вихідної інформації; 2) висування версій та визначення завдань розслідування; 3) визначення шляхів та способів виконання поставлених завдань; 4) складання письмового плану та іншої документації з планування розслідування; контроль виконання та коригування плану розслідування. Отже, через аналіз вихідної інформації, на підставі слідчих ситуацій, що склалися на певних етапах розслідування, плануються дії для виконання поставлених завдань» [37, с. 21].

Інша група науковців (О. В. Узунова, А. В. Логвиненко) відмітила, що «…для успішного подолання існуючих перешкод та приведення проекту

КПК України до стандартів загальновизнаних міжнародних правових принципів, фундаментальних положень кримінального судочинства в демократичних країнах, на нашу думку, необхідно враховувати наступні чинники. В першу чергу, прийняття КПК України затягуватиметься без реформування таких органів як міліція, СБУ, прокуратура й суди. Ні для кого не є секретом, що порядність, професіоналізм, людяність та, врешті решт, патріотизм повинні бути визначальними рисами у кадровому забезпеченні цих органів. По-друге, з цього питання повинна бути вироблена стратегічна лінія поведінки держави, кроки державних органів щодо підготовки проекту КПК України мають бути консолідованими, послідовними та виваженими. По-третє, доцільним залишається проведення різноманітних науковопрактичних конференцій та «круглих столів», де можна було б по-справжньому сперечатися й шукати істину, повноцінно обговорювати недоліки і досягнення проекту КПК України. По-четверте, при розробленні проекту КПК Українинеобхідно дотримуватися балансу приватних та публічних інтересів. Тобто, КПК України повинен як забезпечувати права особи, яка скоїла злочин, так і озброювати слідчого належною процедурою, завдяки якій можна законно розкрити злочин. Поп'яте, потрібно не забувати, що проект КПК України ще потребує доопрацювання та концептуального визначення деяких важливих положень, без яких неможливе взагалі реформування кримінального судочинства» [191].

Згідно з ч. 1 ст. 214 КПК України досудове розслідування розпочинається у таких випадках: «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» [89].

Як слушно зазначав О. Мотлях, комп'ютерні правопорушення мають багато спільного з розслідуванням традиційних видів протиправних діянь, зокрема щодо приводів та підстав початку кримінального провадження. Автор зауважував, що до складу слідчо-оперативної групи, яка виїжджатиме для проведення процесуальних заходів, необхідно долучати штатних співробітників правоохоронних органів, а не запрошених спеціалістів із різних сфер, у тому числі тієї, що досліджується. Автор наголосив, що понятих слід запрошувати не з-поміж працюючого персоналу потерпілих суб'єктів, а зі сторонніх осіб, які хоча б мінімально були б обізнаними з комп'ютерними технологіями. Крім того, науковець запропонував паралельно з традиційними криміналістичними валізами різної комплектації запровадити уніфіковану валізу для розслідування комп'ютерних правопорушень. Як висновок О. Мотлях відмітив, що це дозволить належно провести виявлення і вилучення електронних джерел доказового значення та оперативно направити їх у відповідний науково-дослідний інститут судових експертиз для перевірки та обробки [125, с. 115]. З більшістю позицій автора ми погоджуємося (щодо понятих, уніфікованої валізи для розслідування комп'ютерних правопорушень), але деякі не підтримуємо. Наприклад, стосовно включення штатних співробітників правоохоронних органів, а не запрошених спеціалістів із різних сфер, у тому числі й тієї, що досліджується. Ми вважаємо, що у випадках виявлення розглядуваної категорії протиправних діянь бажано з самого початку залучати відповідних фахівців, в тому числі й зі сфери комп'ютерних технологій.

Відповідно до наказу Генеральної прокуратури № 298 від 30.06.2020 момент внесення інформації 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» [147].

У свою чергу, С. Шапочка зазначав, що розвиток інтернет-технологій, глобальної та локальних мереж дозволили підняти на новий інтернаціонально-континентальний рівень торговельно-економічні відносини та електронну комерцію. Автор акцентує увагу на тому, що еволюціонували, зміцнившись, і позиції транснаціональної злочинності, вони набули нових рис, необмежених можливостей [207, с. 213]. Зі свого боку, С. Самойлов відмітив, що переважно джерелами первинної інформації про вчинення шахрайства будуть: «…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”» [166, с. 84].

Інший автор, А. Рейнгольд визначив такі матеріали початкової перевірки, що підлягають передачі керівникові органу досудового розслідування для внесення до ЄРДР: «…рапорт працівника оперативного підрозділу про виявлення ознак злочину; можливі офіційні матеріали ревізій,

документальних і інших технічних перевірок (ініційованих особою, що повідомила про злочин); матеріали опитування очевидців, свідків, потерпілого тощо (можливі пояснення службових осіб, фахівців банків, підприємств, установ); матеріали перевірки за оперативними, криміналістичними й іншими обліками (в тому числі система Інтерполу I-24/7, захищений канал зв'язку Європолу «SIENA»); протокол огляду, в тому числі як додаткові паперові роздруківки інформації з вилучених машинних носіїв інформації і інформації, що знаходилася на жорсткому диску переносного комп'ютера підозрюваного; офіційні матеріали різних суб'єктів ринку телекомунікаційних послуг, наприклад від операторів і провайдерів телекомунікаційних послуг про зв'язок, абонента, надання телекомунікаційних послуг, отримання послуг, їх тривалість, зміст, маршрути передавання тощо; інструкції, довідки, інші технічні документи і матеріали» [157, с. 21].

На основі аналізу матеріалів кримінальних проваджень нами було сформульовано висновок, що початкові відомості, котрі стали приводом для внесення інформації до ЄРДР за фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, надійшли до відповідних підрозділів правоохоронних органів у такий спосіб:

а) заяви, листи та повідомлення від громадян, які є потерпілими від визначених кримінальних правопорушень – 79 %;

б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене кримінальне правопорушення або були свідками його скоєння – 8 %;

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

г) матеріали досудового розслідування, виділені з інших кримінальних проваджень – 4 %;

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

Так, 03 березня 2021 р. о 01 год. 30 хв. гр. О., маючи доступ до

облікового запису гр. З. в автоматизованій системі е-банкінгу «Приват24», маючи фізичний доступ до раніше викраденої банківської картки АТ КБ «ПриватБанк», використовуючи мобільний телефон, через мережу Інтернет отримав доступ до інформації, що зберігається та обробляється в автоматизованій системі віддаленого доступу е-банкінгу «Приват24», видав себе за потерпілу, що призвело до витоку інформації про клієнта банку, та втрутився в роботу автоматизованої системи е-банкінгу «Приват24», видаючи себе за потерпілу, шляхом подачі електронного документа на переказ грошових коштів – платіжного доручення – здійснив підробку інформації про необхідність проведення грошового переказу, внаслідок чого було проведено онлайн переказ грошових коштів з банківської картки на рахунок онлайн-ігор у сумі 100 грн. Крім того, шахрай вищевказаним способом та з тією самою метою ще декілька разів здійснив перекази на рахунок онлайн-ігор по 100 грн кожного разу, а загалом у розмірі 400 грн [180]. Про вказані факти повідомила потерпіла, коли звернулася до відділення поліції стосовно вчинення щодо неї шахрайських дій.

Стосовно типових слідчих ситуацій, що виникають на початковому етапі розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу, для початку звернемося до окремих праць науковців у розрізі дослідження їх поняття та сутності. Так, І. Попова вказувала, що «…доцільно вирізнити такі, яким відповідає певна сукупність інформації, що її містять матеріали попередньої перевірки на стадії порушення кримінальної справи: 1) матеріали перевірки містять усі необхідні дані про обставини вчинення злочину і є достатніми для порушення кримінальної справи; 2) вихідні дані недостатні для порушення кримінальної справи, оскільки дають змогу припускати як наявність, так і відсутність події злочину (наприклад, виявлення факту зникнення керівників компанії-забудовника або зупинення будівництва без достатніх підстав), що потребує подальшого проведення цільових перевірочних заходів; 3) з наявних даних убачаються ознаки об’єктивної сторони злочину, проте невідомі мотив, мета

та суб’єкт (наприклад, виявлено факт укладання угоди щодо однієї квартири в новобудові з декількома інвесторами; виявлення ознак фіктивності в діяльності компанії-управителя коштів тощо); 4) матеріали не містять достатніх даних для порушення кримінальної справи та не можуть бути доповнені під час проведення додаткових перевірочних заходів або досудового слідства (наприклад, після знищення документів обліку діяльності будівельних організацій; відсутність можливості проведення документальних та інших перевірок тощо); 5) матеріали свідчать про відсутність складу злочину в діях службових осіб (бухгалтерська помилка, фінансова неспроможність унаслідок впливу чинників ризику, цивільно-правові відносини тощо)» [143, с. 12].

А вже Є. Хижняк зауважував, що «…слідча ситуація, як і криміналістична характеристика, є одним із найважливіших інструментів у руках слідчого, що дає змогу максимально підвищити ефективність діяльності з розслідування злочинів, а володіння типовими слідчими ситуаціями дає змогу слідчому визначити коло пріоритетних завдань, уникнути непотрібної витрати часу та сил. 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» [192, с. 197].

Зі свого боку, С. Чернявський визначив типову слідчу як «….інформаційну модель з найбільш значущими властивостями та ознаками процесу розслідування в кримінальних провадженнях щодо злочинів певної категорії» [200, с. 405]. У свою чергу, А. Іщенко та Г. Щербаков засвідчували, що «…вивчення питання слідчої ситуації як криміналістичної категорії має теоретичне та прикладне значення. Теоретичне значення розроблення цієї проблеми в загальному полягає в об’єктивній необхідності конкретизації змісту та поняття цієї наукової категорії. Його практичне

значення 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» [55, с. 57].

Найбільш лаконічним та точним формулюванням вважаємо надане І. Коваленком визначення типової слідчої ситуації як сформованої на підставі аналізу практики розслідування певної категорії кримінальних правопорушень інформаційної моделі з найбільш значущими властивостями та ознаками певної категорії кримінальних проваджень [68, с. 101].

З метою визначення конкретних типових слідчих ситуацій початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, для початку звернемося до праць окремих дослідників. Зокрема, І. Попова з огляду на опрацювання матеріалів судово-слідчої практики за фактом вчинення шахрайства на первинному ринку нерухомості виокремила такі слідчі ситуації: «…1) вчинено шахрайські дії при оформленні документів, необхідних для проведення будівництва, наявна матеріальна і особистісна доказова інформація, виявлена організована група шахраїв – 11 %; 2) вчинено шахрайські дії при оформленні документів, необхідних для проведення будівництва, відсутня достатня доказова інформація – 23 %; 3) вчинено шахрайські дії при безпосередньому укладанні договорів з громадянами щодо будівництва нерухомості, наявна матеріальна та особистісна доказова інформація, виявлена організована група шахраїв – 9 %; 4) вчинено шахрайські дії при безпосередньому укладанні договорів з громадянами щодо будівництва нерухомості, відсутня достатня доказова інформація – 19 %; 5) вчинено шахрайські дії із внесенням навмисних змін у документи, що надають або позбавляють прав певних осіб на отримання житла в новобудові, наявна матеріальна та особистісна доказова інформація, виявлена організована група шахраїв – 4 %; 6) вчинено шахрайські дії із внесенням навмисних змін у документи, що надають або позбавляють прав певних осіб на отримання житла в новобудові, відсутня достатня доказова

інформація – 29 %; 7) інші – 5 %» [144, с. 119].

Зі свого боку, О. Курман виділив такі слідчі ситуації, що формуються під час розслідування шахрайства з фінансовими ресурсами: «…1) слідча ситуація, що характеризується наявністю даних про вчинення шахрайства з фінансовими ресурсами та особу, що вчинила злочин; 2) слідча ситуація, що характеризується наявністю даних про вчинення шахрайства з фінансовими ресурсами та недостатньою кількістю інформації про можливого злочинця. У свою чергу перша слідча ситуація залежно від обсягу і змісту даних, що вказують на чисельність злочинців, може бути розподілена на декілька інших: 1) у вчиненні злочину брало участь декілька осіб з боку позичальника; 2) у вчиненні злочину брали участь позичальник та представник кредитора; 3) злочин вчинено організованою злочинною групою» [99, с. 10].

Як вказує М. Комаров, «…важливим атрибутом є об’єкт атаки, так як атаки на об’єкти різної функціональності і категорійності мають, як правило, різний характер. Тут виділяються такі властивості об’єкта атаки, як тип системи, яку атакують, її фізичний носій (обладнання, яке формує інформаційно-обчислювальну середу системи), тип засобів захисту, які використовуються в системі, і ступінь захищеності (рівень жорсткості правил безпеки), а також зовнішні комунікації системи. Ще одним атрибутом атаки є атакуючий. Основними властивостями, які його характеризують, є розташування щодо системи, початкові привілеї і права доступу. Якщо атакуючих декілька, то в цьому випадку виникає ворожа багатоагентна система, тому стає вкрай важливим їх кількість, наявність і характер координації між атакуючими» [71, с. 96].

З огляду на вищезазначене вважаємо доречним навести позицію С. Кузьменка, який вирізнив декілька слідчих ситуацій початкового етапу розслідування шахрайств, пов’язаних із інвестуванням коштів у будівництво об’єктів нерухомості, а саме: «…1) Кримінальне провадження відкрито за заявою особи (осіб), яка інвестувала кошти у будівництво об’єкта нерухомості, а згодом їй стало відомо, що забудовник заздалегідь не

планував завершувати розпочате будівництво. 2) Кримінальне провадження відкрито за заявою особи (осіб), яка інвестувала кошти у будівництво об'єкта нерухомості, який завершено та здано в експлуатацію. 3) Кримінальне провадження відкрито за заявою представника юридичної особи за фактом незаконної забудови або інших порушень законодавства. У ході розслідування стало відомо про інвесторів, які не здогадувалися, що вклали кошти в будівництво об'єктів нерухомості, яке внаслідок виявилося незаконним. Наявні ознаки вчинення шахрайства, пов'язаного із інвестуванням коштів у будівництво об'єктів нерухомості, але вони не очевидні, слідова картина відносно інформативна, є інформація про можливу причетність до шахрайства певних осіб. 4) Кримінальне провадження відкрито внаслідок самостійного виявлення правоохоронними органами обставин, що свідчать про вчинення обману у відношенні інвесторів при забудові об'єктів нерухомості. 5) Інвестори, які втратили вкладені ними гроші у будівництво об'єктів нерухомості, що внаслідок припинилося, звертаються із заявою про вчинене стосовно них шахрайство. Ознаки шахрайства не є очевидними, оскільки є достатні підстави вважати, що забудовник залишився без джерел фінансування під впливом економічної нестабільності і в силу непередбачених обставин вимушений був припинити будівництво житлових будинків, опинившись на межі банкрутства. 6) Розпочато розслідування за фактом шахрайства, але дії шахраїв завуальовані під виглядом законних цивільно-правових угод» [94, с. 95–100].

Наостанок наведемо твердження О. Мусієнка, який наводить такий перелік слідчих ситуацій: «…ситуації, що виникають у ході перевірки повідомлень і заяв про злочини; ситуації, що виникають при вирішенні питання про порушення кримінальної справи; ситуації, що виникають під час висування та перевірки слідчих версій і планування розслідування; ситуації підготовки та проведення слідчих дій та організаційно-технічних та інших заходів; ситуації забезпечення слідчим взаємодії з органом дізнання, наглядовими й контролюючими органами в розслідуванні злочинів; ситуації

пошукової діяльності слідчого; ситуації зупинення кримінальної справи (по нерозкритому злочину); ситуація поновлення припиненої кримінальної справи; ситуації складання обвинувального висновку (аналіз матеріалів кримінальної справи); ситуації, пов'язані з передачею матеріалів до суду; ситуації, пов'язані із припиненням кримінальної справи» [127, с. 104].

На основі вивчення матеріалів кримінальних проваджень [Додаток А] нами було вирізнено типові слідчі ситуації, що формуються на початковому етапі розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от:

1) вчинено кримінальне правопорушення, пов'язане з використанням е-банкінгу, наявна достатня кількість доказової інформації, встановлено особу злочинця – 7 %;

2) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, особу злочинця не встановлено– 62 %;

3) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, встановлено особу злочинця, але злочинні дії замасковані під легальну фінансову діяльність – 8 %;

4) вчинено кримінальне правопорушення, наявна заява потерпілої особи, відсутня будь-яка доказова інформація – 23 %.

До зазначених ситуацій окреслимо відповідні тактичні завдання, котрі необхідно вирішити у кожній із них. Зокрема, для першої ситуації обов'язковими є збір та перевірка доказової інформації для пред'явлення підозри злочинцю. Для другої ситуації необхідно з огляду на наявну доказову інформацію встановити та затримати правопорушника. У третій варто провести всі можливі процесуальні дії для виявлення способу маскування кримінальних правопорушень під легальну фінансову діяльність. В останній ситуації потрібно провести СРД, НСРД та інші процесуальні дії і пошукові заходи для виявлення доказової інформації.

З огляду на опрацювання анкетування респондентів [Додаток Б] нами було вирізнено тактичні помилки, котрих припускаються слідчі, які

розпочали розслідування:

– прорахунки у діагностуванні злочинної події та визначенні напрямів розслідування – 84 %;

– порушення процесуального порядку проведення СРД – 62 %;

– проведення невідкладних слідчих (розшукових) дій без участі спеціаліста – 57 %;

– ігнорування встановлення низки важливих обставин – 37 %;

– «поверхневий» характер невідкладних слідчих (розшукових) дій (огляд, обшук) – 29 % та ін.

Підсумовуючи, зазначимо, що в кримінальних провадженнях, розпочатих за фактом вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, першочергові заходи загалом обумовлюються відсутністю злочинця на місці події.

2.2. Взаємодія слідчих та працівників оперативних підрозділів Національної поліції України у кримінальному провадженні

Для досягнення оптимальної мети спільної діяльності як окремі індивіди, так і групи осіб повинні чітко співпрацювати. Зазначений процес за своєю суттю є взаємодією між певними суб’єктами, котра реалізується задля досягнення конкретної цілі. Процес розслідування в цьому аспекті характеризується досить специфічною взаємодією залежно від конкретного кримінального правопорушення, за фактом учинення якого було внесено відомості до ЄРДР. Оскільки кожне протиправне діяння відрізняється за багатьма ознаками. Так, із-поміж них варто виокремити: склад кримінального правопорушення відповідно до положень Кримінального кодексу України; особливості проведення окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів; залучення до кримінального провадження відповідних підрозділів правоохоронних органів

тощо. Остання ознака, тісно переплітаючись із іншими, й визначає специфіку взаємодії під час розслідування кримінальних правопорушень будь-якої категорії, зокрема пов’язаних із використанням е-банкінгу [113, с. 232].

Ми поділяємо позицію М. Куратченка, який зауважував, що під час розслідування взаємодія слідчих та оперативних підрозділів є важливою умовою того, що кримінальне провадження буде швидко та ефективно завершено. Автор акцентував увагу на тому, що завдяки злагодженій взаємодії збирається достатня доказова база для проведення подальших процесуальних дій, висуваються оптимальні слідчі версії та планується процес розслідування. Крім того, науковець зазначив, що працівники Національної поліції України повинні реагувати на обставини, що характеризують кожний конкретний момент процесу розслідування, та визначати свої функції залежно від обов’язків. Наостанок дослідник підсумував, що взаємодія різних підрозділів правоохоронних органів займає важливе місце в будь-якому кримінальному провадженні [98, с. 99]. Повністю схвалюємо визначену думку, адже, дійсно, визначена криміналістична категорія має неабияке значення для розслідування кримінальних правопорушень.

Інша група авторів відмічає, що одним із ключових завдань правоохоронних органів є створення ефективної та стабільної системи підготовки фахівців, які володітимуть технологіями розслідування кримінальних правопорушень, пов’язаних із легалізацією (відмиванням) доходів, одержаних незаконним шляхом. Науковці вказують, що з метою недопущення використання зловмисниками доходів, отриманих протиправним шляхом, доцільно застосовувати заходи своєчасного накладення арешту на майно відповідно до справ. Дослідники встановили, що кількість і різноманітність способів інтернет-шахрайства зростає буквально щосекунди, оскільки зловмисники застосовують новітні технології та обладнання, дуже швидко адаптуючи їх до своїх злочинних цілей. Крім того, вчені-криміналісти зауважили, що з-поміж усіх видів інтернет-

шахрайства можна виділити основні та найпоширеніші: фішинг, сніфінг, вішинг, кардинг [221, с. 166–167]. Підтримуючи наведені позиції, зазначимо, що одним із найбільш поширених кримінальних правопорушень, пов'язаних із використанням е-банкінгу, є інтернет-шахрайства. Розслідування зазначених протиправних діянь є важливим напрямом діяльності правоохоронних органів України.

Автор А. Жилін зауважував, що «…взаємодія є обов'язковою складовою для будь-якого соціального процесу. Під час розслідування кримінальних правопорушень вказана категорія не зменшує свого значення, а навпаки, необхідність її застосування лише збільшується. Тим паче в кримінальних провадженнях за фактом вчинення шахрайства у сфері використання банківських електронних платежів. Це пояснюється наступними факторами. Наприклад, завжди виникає потреба у реалізації негласних слідчих (розшукових) дій, що одразу вказує на обов'язкове залучення спеціалістів різних підрозділів правоохоронних органів. Крім того, реалізація окремих тактичних операцій також викликає необхідність у взаємодії не тільки працівників Національної поліції, але й інших відомств» [40, с. 133].

Окрема група науковців, зважаючи на велику суспільну небезпеку окремих категорій кримінальних правопорушень, вказала, що вони вже давно набули транснаціонального характеру, тому слід звернути особливу увагу на питання співпраці Національної поліції України з різними міжнародними поліцейськими організаціями. Дослідники дійшли висновків, що зміцнення взаємодії оперативних підрозділів Національної поліції України, які здійснюють боротьбу з кримінальними правопорушеннями, та органів міжнародної поліції, які здійснюють оперативно-розшукову діяльність, є обов'язковою умовою можливості протидії злочинності в усіх її проявах. Крім того, автори наголосили на тому, що з-поміж розповсюджених помилок науковцями було виокремлено ті, що пов'язані з неправильною організацією та плануванням слідчих (розшукових) дій та інших процесуальних дій,

інформаційною складовою яких є отримання результатів оперативно-розшукової діяльності [217]. Погоджуючись зі вказаною позицією, зауважимо, що правильно спланована та організована взаємодія різних підрозділів правоохоронних органів забезпечить максимальне отримання доказової інформації для найбільш ефективного проведення процесуальних дій і заходів.

Зі свого боку, О. Саінчин зазначає такі загальні умови взаємодії: найсуворіше дотримання законності; плановість; швидкість, активність і широке застосування науково-технічних засобів у ході розслідування; обов'язкове залучення громадськості; правильне ставлення до оцінки доказів; знання кожним учасником взаємодії повноважень і форм діяльності органів слідства і дізнання; точне розмежування компетенції учасників взаємодії; врахування провідної ролі уповноваженої особи в процесі взаємодії; нерозголошення даних досудового розслідування, а також засобів і методів, застосовуваних в ОРД [160, с. 267].

Стосовно визначення поняття досліджуваної криміналістичної категорії зазначимо, що, наприклад, І. Козаченко та В. Регульський сформулювали взаємодію слідчих та оперативних підрозділів як «…концентрацію сил, засобів і методів для досягнення поставленої мети, здійснення відповідних спільних заходів, вибору таких тактичних прийомів або їх комбінацій, які найкраще забезпечують виконання завдань у винятково короткі терміни силами і засобами, що є в розпорядженні суб'єктів взаємодії, при найменших витратах і при безумовному дотриманні чинного законодавства» [69, с. 179]. У свою чергу, Г. Душейко визначає її так: «…правильне (або раціональне) поєднання та ефективне використання повноважень, методів і форм діяльності слідчого й оперативних підрозділів» [32, с. 12]. Тобто правильно спланована й організована взаємодія різних підрозділів Національної поліції України забезпечить отримання достатньої доказової інформації для найбільш ефективного проведення процесуальних дій та розшукових заходів.

На нашу думку, взаємодія правоохоронних органів – це спільна й взаємообумовлена діяльність окремих підрозділів Національної поліції України, визначена нормативно-правовою базою, а також погоджена за ціллю, місцем і часом функціонування окремих підрозділів, що виявляється в оптимальному проведенні ними спільних заходів, що мають ціллю запобігання та розслідування протиправних діянь.

З приводу форм взаємодії М. Погорецький підкреслював, що вони «…поділяються на процесуальні, які врегульовані кримінально-процесуальним законом, та організаційно-тактичні (непроцесуальні), що врегульовані відомчими нормативними актами (наказами, інструкціями, вказівками), а також нормами службової етики та вироблені практикою» [141, с. 179]. Провівши ґрунтовний аналіз наукових поглядів стосовно форм взаємодії уповноваженої особи з іншими суб'єктами взаємодії, О. Самойленко дійшла висновку, що існують такі підстави для їх класифікації: «…1) нормативно-правова регламентація: а) процесуальні форми (передбачені КПК України): надання доручень співробітникам оперативних підрозділів щодо проведення С(Р)Д та НС(Р)Д (ч. 3 ст. 39, ч. 4 ст. 40, ч. 3 ст. 41 КПК України); залучення до участі в процесуальній дії співробітників оперативних підрозділів як спеціалістів чи інших учасників кримінального провадження, залучення інших спеціалістів, які мають спеціальні знання та навички (психологи, перекладачі), зокрема під час огляду місця події, обшуку, одержання зразків для експертизи тощо (ст. ст. 40, 228, 236, 237 та інші); б) непроцесуальні (організаційно-тактичні) форми: створення слідчо-оперативних груп (тимчасових чи постійно діючих); забезпечення слідчим методичного супроводження ведення ОРС; залучення співробітників до забезпечення організаційних умов проведення охорони, конвоювання, затримання тощо; спільне планування слідчих (розшукових) та негласних слідчих (розшукових) дій, розслідування в цілому; взаємний обмін інформацією; поєднання узгоджених спільних дій та заходів кримінального провадження; обмін інформацією; залучення

громадськості до участі у проведенні процесуальних дій та організаційних заходів); 2) рівень взаємодії: а) міжнародна взаємодія; б) міжвідомча взаємодія; в) внутрішньовідомча взаємодія (між різними підрозділами одного відомства); 3) стадія кримінально-процесуальної діяльності: а) взаємодія до початку кримінального провадження (в рамках ОРС та під час попередньої перевірки інформації про злочин); взаємодія в ході здійснення досудового розслідування; б) взаємодія на стадії судового розгляду» [164, с. 185].

Доречними також вважаємо результати дисертаційного дослідження, проведеного О. Бойком, який у межах нього дійшов висновку, що з-поміж процесуальних форм взаємодії варто виділити такі: «…під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій за дорученням слідчого; при застосуванні заходів забезпечення кримінального провадження; при оголошенні в розшук підозрюваного». Крім того, дослідник окреслив і непроцесуальні форми взаємодії, а саме: «…взаємне інформування; надання інформації при отриманні необхідних відомостей; спільний аналіз при отриманні інформації; спільне планування оперативно-розшукових заходів, а також слідчих (розшукових) дій; консультації; взаємодію у разі направлення матеріалів за результатами оперативно-розшукової діяльності; спільний аналіз причин та умов, які сприяють вчиненню кримінального правопорушення, та обговорювання оперативно-профілактичних заходів; досудове розслідування у складі слідчо-оперативних груп; проведення оперативних нарад щодо проблемних питань взаємодії; аналіз за результатами проведення спільних дій у конкретних кримінальних провадженнях; надання допомоги наявними силами й засобами; підбиття підсумків спільної діяльності з метою усунення недоліків та підвищення ефективності здійснення взаємодії у майбутньому» [16, с. 14–15]. Як бачимо, така діяльність здійснюється під єдиним керівництвом, що зводиться до здійснення усіх СРД, НСРД та розшукових заходів у чіткій співпраці та координації з метою найбільш швидкого й ефективного досягнення та вирішення завдань конкретного кримінального провадження.

Інший автор, Д. Никифорчук вирізняє такі форми взаємодії: «…здійснення самостійно органами дізнання оперативно-розшукових заходів і термінове інформування слідчого про результати; виконання органами дізнання оперативно-розшукових заходів і невідкладних слідчих дій за дорученням слідчого; виконання органами дізнання вимог слідчого, із метою сприяти виконанню слідчих дій; виконання органами дізнання доручень на проведення слідчих дій в інших районах; виконання оперативними підрозділами запитів відповідних міжнародних правоохоронних організацій та правоохоронних органів, запитів повноважних державних органів, установ та організацій щодо проведення оперативно-розшукових заходів; здійснення органом дізнання розшуку обвинуваченого згідно з дорученням слідчого; участь спеціалістів правоохоронних органів у проведенні слідчих дій; проведення експертиз в експертних установах органів внутрішніх справ; застосування заходів безпеки стосовно осіб, які беруть участь у кримінальному судочинстві і проходять за кримінальною справою, що знаходиться у провадженні слідчого чи органу дізнання; проведення оперативно-розшукових заходів відносно осіб, затриманих за вчинення злочину, та осіб, взятих під варту» [130, с. 154].

Здійснивши аналіз окремих форм взаємодії, О. Самойленко вказала на наявність таких суб’єктів взаємодії уповноваженої особи під час розслідування кримінальних правопорушень, вчинених у кіберпросторі: «...1) державні органи…: спеціально уповноважені державні органи у сфері телекомунікацій, зокрема орган виконавчої влади з питань організації спеціального зв’язку та захисту інформації…; орган державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, що здійснює також повноваження органу ліцензування, дозвільного органу, регуляторного органу й органу державного нагляду (контролю)…; Національна рада України з питань телебачення і радіомовлення; Державне підприємство «Український державний центр радіочастот»; Національний банк України; 2) громадські

об’єднання/організації…; 3) суб’єкт господарювання (оператори та провайдери) у сфері зв’язку та телекомунікацій…; 4) комерційні банківські установи, суб’єкти господарювання у сфері платіжних систем…; 5) засоби масової інформації…; 6) міжнародні правоохоронні організації…; 7) інші власники (розпорядники) систем та володільці інформації» [163, с. 409–410].

Зі свого боку, провівши власне дослідження взаємодії слідчих та оперативних працівників під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет, С. Чучко виокремив рівень діяльності служб і підрозділів, а також рівень розслідування окремого кримінального провадження. Науковець із приводу вказаних рівнів дійшов таких висновків: «…на першому рівні – це, насамперед, підготовка і розподіл висококваліфікованих кадрів слідчих і оперативних працівників, здатних успішно виявляти, розслідувати кримінальні правопорушення у досліджуваній сфері, вчинені з використанням різних способів, в умовах активної, у тому числі організованої, протидії з боку правопорушників і пов’язаних з ними осіб» [204, с. 204]. Тобто необхідно з’ясувати особливості взаємодії уповноважених осіб (слідчих, дізнавачів, прокурорів, детективів) із іншими працівниками правоохоронних органів, а також різних установ, підприємств та організацій, громадськістю тощо.

Так, С. Самойлов, опрацьовуючи питання особливостей отримання відомостей від установ та організацій під час розслідування шахрайств, учинених із використанням мережі «Інтернет», зауважував на потребі застосування цього способу отримання доказових даних. На думку автора, його ефективність напряму залежить від того, наскільки уповноважена особа тактично правильно підготує вказаний запит, чому допомагає додержання таких умов: а) своєчасності запиту; б) законності запиту; в) визначення вичерпного переліку інформації, яку варто з’ясувати шляхом запиту. Крім того, дослідник визначив, що залежно від обставин учинення протиправного діяння окремі запити направляють до: а) адміністрації відповідного сервісу або ресурсу, на якому і було вчинено шахрайські дії; б) постачальника

послуги підключення до мережі Інтернет (провайдера). Також науковець розгорнуто проаналізував перелік відомостей, котрі можна отримати у такий спосіб, та порадив окрему форму запиту з урахуванням специфічності інформації [165, с. 258].

Цікавою є позиція колективу авторів під керівництвом В. В. Чернея, які з-поміж організаційних форм взаємодії виділили такі: «…обмін оперативною і іншою інформацією; спільне планування, узгодження за часом та місцем та здійснення оперативно-розшукових заходів; допомога наявними силами та засобами; тимчасова передача негласних співробітників; обмін досвідом оперативно-розшукової діяльності; проведення спільних оперативно-тактичних операцій; ...спільне видання оглядів, методичних рекомендацій за результатами спільної діяльності у протидії злочинності» [124, с. 1044].

Опрацювання результатів анкетування респондентів [Додаток Б] дало змогу виокремити найбільш розповсюджені форми взаємодії при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу, як-от:

– здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів – 91 %;

– обмін інформацією – 83 %;

– надання уповноваженій особі відомостей, що зібрані у процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення інформації до ЄРДР – 65 %;

– групове планування оперативно-розшукових заходів – 31 %;

– здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, що мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними матеріалами – 29 %.

Слід наголосити на важливості використання обміну інформацією як однієї з найбільш ефективних форм взаємодії, особливо в умовах

запровадженого воєнного стану. Щодо її застосування ми підтримуємо позицію М. Єфімова, який акцентував увагу на тому, що обмін інформацією «…може стосуватися: а) ознак кримінальних правопорушень проти моральності (вчинених чи тих, що готуються); б) фізичних і юридичних осіб, причетних до кримінальних правопорушень, а також потерпілих осіб; в) складу, структури, сфери діяльності та зв'язків ОГ і ЗО; г) предметів, які є предметом злочинного посягання, складають інтерес для розслідування (тварини; предмети порнографічного характеру; твори, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість і дискримінацію; документи Національного архівного фонду; тіло (останки, прах) померлого; урна з прахом померлого); д) слідів кримінальних правопорушень проти моральності, речових доказів, які можуть сприяти з'ясуванню обставин розслідуваних кримінальних правопорушень (матеріали ДНК; вилучені відбитки слідів пальців рук), тощо» [34, с. 211].

У межах нашого дослідження слід вказати, що наведена інформація може стосуватися таких обставин:

а) ознак злочинного діяння, пов'язаного з використанням е-банкінгу (котре вчинене або знаходиться на етапі підготовки);

б) структури ОГ та ЗО, що здійснюють тривалу злочинну діяльність в економічній сфері;

в) характерних ознак злочинців (хакерів, спамерів, фішерів, фрікерів, кіберсквотерів, лідерів ОЗГ та їхніх членів), які здійснюють протиправну діяльність).

На основі опитування респондентів [Додаток Б] серед типових недоліків у процесі реалізації взаємодії вказаних підрозділів під час розслідування кримінальних правопорушень, вчинених із використанням е-банкінгу, слід зазначити такі, як:

– здійснення СРД, НСРД та інших процесуальних дій оперативними працівниками без участі уповноваженої особи – 41 %;

– невчасний початок здійснення взаємодії – 78 %;

– спрямування початкових СРД, НСРД та інших процесуальних дій на досягнення «визначальної» мети – затримання правопорушника, в той час як реалізація встановлення обставин вчинення кримінальних правопорушень із використанням е-банкінгу відходить на другий план – 53 %;

– припинення взаємодії з боку учасників кримінального провадження після закінчення його початкового етапу – 69 %.

Стосовно вказаного вбачаємо слушною позицію Д. Безрукова, який зауважував: «…підвищити рівень інформаційного забезпечення щодо протидії злочинам проти власності можна за рахунок використання: глобальних телекомунікаційних мереж; багатофункціональних систем реєстрації документування, зберігання і відтворення мовленнєвої інформації і зображень телефонними (аналоговими, цифровими), радіо-, відео- та іншими каналами зв'язку; нових сервісів стільникових операторів (місце розташування абонента за номером стільника); геолокаційних Інтернет-телекомунікаційних сервісів («FourSquare»); соціальних мереж; веб-камер; мобільних систем безпеки (3rd-i) тощо» [7, с. 11].

Крім того, В. Іванов вказував, що «…необхідність взаємодії слідчого та оперативних працівників в процесі розслідування пояснюється наступними обставинами: різницею засобів і методів здійснення діяльності слідчого й оперативного працівника. Справа в тому, що слідчий здійснює свою діяльність засобами і методами, врегульованими кримінально-процесуальним правом, які носять гласний характер. Оперативні працівники здійснюють оперативно-розшукову діяльність у межах, окреслених законом «Про оперативно-розшукову діяльність», і засоби й методи, що ними застосовуються, носять переважно негласний характер та відкривають принципово інші, більш широкі можливості, у порівнянні із процесуальними діями по одержанню фактичних даних, що мають значення для повного і швидкого розкриття та розслідування злочинів» [54, с. 19].

Також варто наголосити на обов'язковій взаємодії уповноважених осіб з працівниками різних підрозділів Департаменту кіберполіції для

ефективного здійснення визначеної категорії кримінальних проваджень.

Так, гр. Ж. 10.09.2021 приблизно о 23 год. 00 хв., знаходячись біля магазину «Діжка», що на вулиці Львівській у м. Стрий Львівської області, попросив свою знайому гр. Ю. взяти мобільний телефон у гр. Ф. під приводом необхідності здійснення дзвінка. Після того, як остання, з дозволу потерпілого, отримала в своє тимчасове користування мобільний телефон, вона передала його правопорушнику, який, відійшовши в сторону, непомітно для всіх витягнув зі вказаного мобільного телефону сім-картку, та в цей час у гр. Ж. виник умисел, направлений на здійснення незаконних операцій з використанням ЕОТ. Після чого правопорушник повернув телефон своїй знайомій, яка передала його потерпілому. Надалі правопорушник 10.09.2021 в період з 23 год. 00 хв. до 23 год. 54 хв., перебуваючи поблизу магазину «Діжка», маючи в тимчасовому користуванні належну потерпілому сім-карту, вставив її у свій мобільний телефон марки та завантажив додаток «Приват24», що є е-банкінгом, системою, призначеною для дистанційного керування банківськими рахунками банку «ПриватБанк», створив особистий кабінет потерпілого в автоматизованій системі ПАТ КБ ПриватБанк «Приват24», без згоди та відома останнього. Надалі правопорушник, із метою заволодіння чужим майном, через мобільний додаток «Приват24», який був встановлений на його мобільному телефоні, діючи від імені потерпілого, увійшов у додаток «Приват24» та отримав доступ до коштів, розміщених на рахунках, і відомостей про персональні дані гр. Ф., реквізитів офіційних документів останнього, що надало можливість здійснювати операції з оформлення кредитних зобов’язань від його імені. Таким чином, гр. Ж. отримав у своє повне розпорядження систему дистанційного керування банківськими рахунками потерпілого. У подальшому, 10.09.2021 приблизно о 23 год. 54 хв., перебуваючи поблизу магазину «Діжка», правопорушник, використовуючи власний мобільний телефон, маючи доступ до е-банкінгу потерпілого, за допомогою програми «Приват24» створив пароль для доступу до е-банкінгу. Після цього він із використанням

створеного ним паролю перевів кошти на картку своєї знайомої [177]. Завдяки взаємодії з працівниками кіберполіції та допомозі останніх за дорученням слідчого було встановлено місцезнаходження мобільного телефону, з якого було вчинено протиправні дії, а надалі й місцезнаходження правопорушника.

Зважаючи на вищезазначене, варто зауважити, що «…кіберполіція (Департамент кіберполіції Національної поліції України) – міжрегіональний територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних Інтернет-мереж і систем» [61].

Окрема група авторів (М. Єфімов, Н. Павлова, С. Чучко) слушно наголошує на тому, що «…серед обов'язків працівників цієї структури є розслідування правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а також загалом правопорушень, які вчиняються за допомогою комп'ютерних технологій. Зокрема, шахрайство, передбачене ч. 3 ст. 190 КК України, та заволодіння коштами громадян через Інтернет-аукціони, Інтернет-магазини, сайти та телекомунікаційні засоби зв'язку» [36, с. 124].

Наостанок наведемо позицію С. Чернявського, який зазначав, що «…взаємодія у протидії злочинності – це узгоджена діяльність уповноважених суб'єктів з оптимальним співвідношенням методів і засобів, визначених для кожного з них. Визначено, що на етапі розкриття фінансового шахрайства взаємодія слідчого та оперативних підрозділів відбувається у процесуальних і непроцесуальних формах. До процесуальних належать: спільна перевірка

інформації про злочин; створення слідчо-оперативної групи; проведення оперативно-розшукових заходів у справах, де не встановлено особу, яка вчинила злочин; виконання доручень слідчого про проведення оперативно-розшукових заходів та слідчих дій. Найбільш ефективними непроцесуальними формами взаємодії є: надання слідчим консультацій щодо повноти збирання матеріалів на стадії порушення кримінальної справи; спільне планування заходів з розкриття злочинів; обмін інформацією за результатами проведених слідчих дій та оперативно-розшукових заходів; забезпечення безпеки учасників кримінального судочинства. Встановлено, що форми передачі та критерії відбору оперативно-розшукової інформації, яка надходить до слідчого, ще належним чином не відрегульовано. Опитані слідчі підтвердили, що доказову інформацію отримують від оперативних працівників переважно в усній формі (58,6 %). Ініціаторами її використання в доказуванні, зазвичай, є оперативний працівник (71,4 %) чи керівництво оперативного підрозділу (26,9 %). Близько 75,0 % оперативних працівників не повідомляють слідчим здобуті дані, що мають значення у справі, оскільки, на їх думку, слідчий не має достатніх фахових знань і не зуміє правильно їх використати, а 36,9 % опитаних повідомляють лише ті дані, які запитує слідчий. Натомість 12,0 % опитаних слідчих переконані, що важлива оперативно-розшукова інформація до них узагалі не надходить, а 64,0 % вважають, що надходить запізно. Мабуть, тому 40,0 % слідчих уважають неналежне оперативно-розшукове забезпечення передумовою низької ефективності досудового слідства. Ці тенденції підтверджено результатами вивчення кримінальних справ (лише 15,0 % справ містили посилання на дані, здобуті оперативним шляхом; у 62,0 % справ не вжито жодних оперативно-розшукових заходів щодо перевірки участі фігурантів у вчиненні інших злочинів)» [199, с. 17].

Констатуючи вищенаведене, зазначимо, що правильно спланована та організована взаємодія різних підрозділів правоохоронних органів забезпечує отримання доказової інформації у максимальному обсязі, необхідному для найбільш ефективного проведення процесуальних дій і заходів.

2.3. Профілактична діяльність уповноважених осіб у кримінальних провадженнях за фактами вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу

Запобігання протиправним діянням із кожним роком стає все більш важливим напрямом діяльності всіх підрозділів правоохоронних органів у демократичних державах. У кримінальних провадженнях, розпочатих за вчиненими правопорушеннями, пов'язаними із використанням е-банкінгу, профілактичні заходи відіграють неабияку роль. Оскільки правильно організовані дії щодо їх реалізації можуть розбити вщент усі намагання злочинців, які скоюють визначені протиправні діяння. Тому дослідження вказаної проблематики ми вважаємо наразі досить актуальним [119, с. 456].

Усі протиправні діяння, пов'язані з використанням е-банкінгу, вчинюються у кіберпросторі. Стосовно визначення кіберпростору, наприклад, О. Довженко зауважував, що вказана категорія нині набуває все більшого значення для людства, оскільки вона відкриває нові можливості, тому слід очікувати її подальшого розширення. Крім того, автор відмічає, що кіберзлочин відрізняється від звичайного кримінального правопорушення тим, що існує в кібернетичному світі. Також науковець зазначає, що за допомогою кіберпростору можливі практично будь-які види протиправного впливу, що можуть бути охарактеризовані в категоріях звичайного злочину, аж до нанесення тілесних ушкоджень чи вбивства. Тому дослідник робить висновок, що саме використання віртуального простору кіберсвіту відділяє кіберзлочини від подібних їм протиправних діянь, що відбуваються в матеріальному просторі [28, с. 82]. Отже, О. Довженко основною характеристикою кіберзлочинів означив їх вчинення в кіберпросторі. Е-банкінг також має зазначену ознаку, що є визначальною серед інших притаманних йому характеристик.

А вже А. Микитчик відмічає, що «…активний розвиток комунікаційних

мереж, інформаційних технологій і масової комп’ютеризації призвели до еволюційних змін кримінального середовища не тільки на рівні окремих держав, а й у всьому світовому співтоваристві. Відсутність належного соціального контролю призвела до того, що мережа Інтернет практично безкарно стала використовуватися злочинцями як місце і основний засіб вчинення різних протизаконних посягань, як традиційних (шахрайств, крадіжок), так і інших – викрадень та продажу конфіденційної інформації, вимагань, «геймерських» шахрайств, а так само поширення предметів і послуг, які були виключені з легального обігу (наркотичних засобів, дитячої порнографії). Особливу небезпеку становлять кіберекстремізм і крайня його форма – кібертероризм, тобто дії з дезорганізації роботи інформаційних систем, що створюють небезпеку загибелі людей, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків, якщо вони вчинені з метою порушення громадської безпеки, залякування населення або здійснення впливу на прийняття рішення державними органами, а також погроза вчинення зазначених дій з тією ж метою» [123, с. 137]. З огляду на наведену інформацію слід наголосити на тому, що ефективна протидія злочинним проявам у сфері використання банківських електронних платежів вимагає від правоохоронних органів не тільки збирання доказової інформації, але й забезпечення певної профілактичної функції. Тому одним із основних напрямів організації розслідування кримінальних правопорушень є вжиття ефективних заходів щодо запобігання їм.

Доречним також вважаємо судження Л. Шеллі, який зауважував, що правоохоронні органи в окремих країнах не можуть найняти або утримувати персонал, необхідний для боротьби зі злочинною діяльністю транснаціональних злочинних груп. Оскільки, на думку автора, низькі зарплати та корумпованість правоохоронних органів призводять до того, що люди з високорозвиненими технічними навичками не можуть знайти бажану роботу в державному секторі. Дослідник вказував, що комп’ютерні експерти в

країнах, що розвиваються, вирішують не працювати за низьку зарплату в правоохоронних органах, натомість вони працюють у приватному секторі, а інші свідомо чи несвідомо працюють на злочинні та терористичні групи. Тому у деяких країнах, навіть якщо держава виплачує адекватну заробітну плату, державний правоохоронний сектор може не бути законною альтернативою кримінальному сектору, позаяк інституціоналізована корумпованість більшої частини правоохоронних органів та їхні тісні зв'язки з кримінальним сектором у деяких регіонах світу означають, що злочинці можуть платити за спеціалістів як в уряді, так і поза ним. На основі вищевказаного науковець доходить висновку, що у розвинутих країнах відчувається дефіцит кадрів із відповідними навичками інформаційних технологій, адже багато з тих, хто працює у вказаному секторі в Європі та Сполучених Штатах, є іммігрантами зі вказаних країн [219, с. 305]. Окреслена проблема, на нашу думку, є досить актуальною й для України. Оскільки заробітна плата в державних структурах не відповідає відповідним посадам у приватних організаціях. І цей аспект досить жорстко відбивається на можливостях реалізовувати профілактичні заходи під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Зважаючи на наведену тезу, вбачаємо досить вдалою думку групи авторів, які відмічають, що одним із ключових завдань правоохоронних органів є створення ефективної та стабільної системи підготовки фахівців, які володітимуть технологіями розслідування кримінальних правопорушень, пов'язаних із легалізацією (відмиванням) доходів, одержаних незаконним шляхом. Науковці вказують, що інтернет-користувачам, власникам банківських карток і будь-яким звичайним громадянам необхідно знати сучасні методи інтернет-шахрайства. Зокрема, дослідники наголошують на тому, що варто бути дуже обережними при користуванні е-банкінгом, мобільним зв'язком, зі здійсненням покупок в інтернет-магазинах, особливо розкриваючи свої персональні дані під час введення інформації у форми на різних вебсайтах [221, с. 166–167]. Тобто профілактика кримінальних

правопорушень, вчинюваних у кіберпросторі, є завданням працівників правоохоронних органів крізь призму роз'яснення їхньої небезпечності пересічним громадянам.

У свою чергу, А. Микитчик, досліджуючи кіберзлочинність в Україні, дійшов таких висновків: «…кібезлочинність є різновидом злочинності, яка існує нарівні з насильницькою, корисливою, корупційною, екологічною та іншими видами; тісно взаємопов'язана з іншими видами злочинності, оскільки злочини в сфері комп'ютерних технологій доволі часто виступають способом вдосконалення інших кримінальних правопорушень (крадіжка, вимагання, шахрайство та ін.); має високотехнологічний характер, що викликано використанням ІТ-технологій, інформаційно-телекомунікаційних мереж, комп'ютерних пристроїв, носіїв комп'ютерної інформації та інше, які виступають знаряддями і засобами вчинення кримінальних правопорушень; мають високий ступінь латентності, яка становить від декількох десятків до декількох тисяч відсотків з різних видів злочинних діянь, що обумовлено різними об'єктивними факторами (небажання жертв комп'ютерних злочинів звертатися до правоохоронних органів, неочевидність комп'ютерних злочинів для більшості населення в силу їх вчинення у віртуальному середовищі, складність виявлення комп'ютерних злочинів за відсутності необхідної кількості фахівців в правоохоронних органах та ін.); носить високоорганізований характер і тісно взаємопов'язана з організованою злочинністю, так як значна кількість кіберзлочинів (DDoS-атаки, Е-банкінг, фішинг, створення ботів та ін.) вчиняється злочинними групами; має «професійний» характер, так як особи, які вчиняють кіберзлочини, мають злочинну спеціалізацію, не вчиняючи інших видів злочинних діянь; отримують злочинний дохід (прибуток) в результаті злочинної діяльності; мають необхідні знання, вміння, навички в сфері ІТ-технологій для вчинення злочину; дотримуються певних правил, законів, понять і термінології, що дозволяють їм спілкуватися, обмінюватися досвідом і знаходити однодумців; характеризується транскордонністю, так як кіберпростір існує поза

державними кордонами і, будучи загальнодоступним, дозволяє злочинцю, що знаходиться на території однієї держави, вчиняти злочинні дії щодо осіб, які перебувають в іншій державі; носить транснаціональний характер, так як кіберзлочинці в силу своєї приналежності до комп'ютерного «андеграунду» для отримання злочинних доходів та спрощення вчинення злочинних діянь на території двох і більше держав змушені, незалежно від національності, об'єднуватися в міжнародні злочинні групи; знаходиться в стані динамічного розвитку, що обумовлено постійним вдосконаленням існуючих і створенням нових ІТ-технологій, залученням до інформаційних відносини нових учасників, розширенням кіберпростору за рахунок збільшення числа користувачів мережі Інтернет, мобільних комп'ютерних пристроїв, переходом до електронного документообігу все більшої кількості організацій, підприємств, установ; отримала риси економічної злочинності, так як більшість кіберзлочинів відбувається в банківсько-фінансовому або корпоративному секторі (інтернет-банкінг, банківський фішинг, кібервимагання та ін.), а діяльність злочинців спрямована на вилучення доходів (прибутку); трансформується в злочинність політичного характеру, що пов'язано з активізацією протиправної діяльності в кіберпросторі представників хакерського руху, спецслужб і силових структур зарубіжних держав, міжнародних екстремістських і терористичних організацій (DDoS-атаки на урядові сайти, кібершпіонаж щодо інформаційних ресурсів органів державної влади, правоохоронних органів, підприємств оборонно-промислового комплексу, дипломатичних представництв та інше)» [123, с. 137–138]. Тобто дослідник виокремив е-банкінг, що вчиняється злочинними групами та має «професійний» характер, адже особи, які вчиняють кіберзлочини, мають злочинну спеціалізацію, не вчиняючи інших видів протиправних діянь.

Із приводу профілактичних заходів в цілому М. Єфімов та Є. Омаров вказують на те, для підвищення ефективності профілактичної діяльності уповноважених осіб при розслідуванні протиправних діянь необхідно

закріпити у Кримінальному процесуальному кодексі України їхній обов'язок виявляти під час дізнання, досудового слідства та судового розгляду причини й умови, що сприяли вчиненню кримінальних правопорушень, а також вносити до відповідного державного органу, громадської організації або посадової особи подання стосовно вжиття заходів для усунення вищезазначених умов і причин [220, с. 118]. А вже О. Антонюк зауважував, що виявлення та усунення причин та умов, що сприяють вчиненню кримінальних правопорушень, були передбачені як обов'язок працівників правоохоронних органів Кримінально-процесуальним кодексом України до 2012 року. Крім того, автор зазначив, що з прийняттям чинного Кримінального процесуального кодексу України вказану норму з нього видалили. Проте вказаний аспект, на думку науковця, є недоречним, оскільки уповноважені особи в ході здійснення кримінального провадження ознайомлюються з обстановкою вчинення кримінального правопорушення та можуть надати ґрунтовні рекомендації і вказівки щодо усунення вказаних причин та умов [2, с. 177].

Зі свого боку, В. Шемчук наголошував на тому, що «..підготовка пропозицій стосовно врегулювання на законодавчому рівні питання щодо: розмежування кримінальної відповідальності за злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; підвищення рівня відповідальності посадових осіб державних органів, установ та організацій за порушення вимог щодо інформування в установленому порядку про несанкціоновані дії (кібератаки) стосовно державних інформаційних ресурсів; визначення Держспецзв'язку органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів; встановлення обов'язкового погодження з ним завдань (проектів) Національної програми інформатизації, проектів (завдань) створення і розвитку інформаційно-телекомунікаційних систем державних органів, підприємств, установ та організацій державної форми власності» є беззаперечно важливою в розрізі

удосконалення чинного законодавства [210, с. 122]. Наведені позиції ми однозначно підтримуємо, оскільки вказаний обов'язок забезпечить постійну реалізацію відповідних профілактичних заходів. Тобто в чинний Кримінальний процесуальний кодекс необхідно ввести норму, в якій буде зазначено про обов'язок працівників правоохоронних органів (слідчих, дізнавачів, детективів, прокурорів) забезпечувати усунення причин та умов, що сприяли вчиненню протиправних діянь.

З огляду на зазначене важаємо слушним твердження групи дослідників (Т. Діброва, Д. Пісенко, Н. Сметаніна), які зауважили: «…дійсно, можна констатувати підвищення ефективності боротьби з кіберзлочинністю за допомогою посилення відповідальності за наведені кримінальні правопорушення. Розширення меж діяльності правоохоронних органів щодо розслідування кіберзлочинів, посилення санкцій, додаткова криміналізація окремих діянь – стримують потенційних шахраїв, проте проблема постає в тому, що кримінологічні дослідження у більшості випадків спираються на облікові дані злочинності, при цьому відсутнє вивчення соціальних, економічних, політичних, демографічних, організаційних та інших причин кібершахрайства. Пропозицією постає масштабне, глибоке дослідження проблеми з метою розробки більшого кола заходів із протидії кібершахрайству. Необхідно інформувати населення про витончені методи шахраїв, аби не тільки попереджати вчинення нових кримінальних правопорушень, але й виявляти потенційних злочинців» [27, с. 547].

Поняття профілактики протиправних діянь як криміналістичної категорії окремі дослідники визначають по-різному. Зокрема, В. Шепітько розглядає її як «…комплекс заходів, спрямованих на виявлення, обмеження, усунення чи нейтралізацію криміногенних факторів, які детермінують злочинність у цілому й окремий злочин ще до того, як вони призведуть до суспільно небезпечних діянь чи наслідків. Профілактика злочинності – діяльність, здійснювана на ранніх стадіях виникнення та формування в особи намірів здійснення подальшої протиправної діяльності» [211, с. 171].

Окрема група дослідників (Ю. Александров, А. Гаврилишин, О. Джужа) вказала на те, що «…разом з тим практика протидії злочинності свідчить, що при визначенні поняття «профілактики злочинів» потрібно виходити з економічних, соціально-політичних, моральних, психологічних, правових та інших більш широких позицій. Такий підхід дає можливість сформулювати це поняття у широкому розумінні, що включає в себе різні заходи державних органів і громадських організацій. Йдеться про те, щоб не допустити існування злочинності у майбутньому, а у найближчій перспективі – якомога більше обмежувати її прояви. Профілактика злочинності є сформованою системою дій стосовно антисуспільних явищ та їх причинного комплексу з метою розширення тенденції зниження рівня і масштабів злочинності і знешкодження її коріння. Отже, профілактика злочинності розглядається як соціально-правовий процес, що знижує, обмежує, ліквідує явища, породжені злочинністю. У найбільш узагальненому вигляді профілактика злочинності забезпечується усією сукупністю заходів, що здійснюються державними органами і громадськими формуваннями, спрямованими на удосконалення суспільних відносин» [92, с.34].

У свою чергу, інша група науковців (Л. Тюптя, І. Іванов) засвідчує, що «…профілактика – це технологія соціальної роботи, що являє собою комплекс взаємопов’язаних заходів, спрямованих на попередження соціальних проблем, соціальної дисгармонії, соціальних наслідків тиску на особистість складних умов життя, негативних умов соціалізації» [190, с. 215].

Підсумовуючи, надамо авторське визначення профілактики протиправних діянь як спеціального різновиду правоохоронної діяльності, що складається з конкретної сукупності певних дій та заходів, котрі реалізують працівники правоохоронних органів (слідчі, дізнавачі, детективи, прокурори), та має метою усунення причин і умов скоєння окремих категорій кримінальних правопорушень.

Доречною вважаємо думку О. Джужи, який відмічає, що предметом профілактики протиправних діянь є такі елементи: «1) поняття

профілактичної діяльності; 2) види, форми, рівні профілактичної діяльності; 3) суб'єкти і об'єкти профілактичної діяльності; 4) організаційні і правові основи профілактичної діяльності; 5) тактика і методика здійснення профілактичних заходів; 6) особливості профілактики окремих видів злочинів» [148].

Досить правильно В. Приловський наголошує на тому, що профілактична діяльність є засобом попередження вчинення кримінальних правопорушень у майбутньому. З огляду на зазначене автор зауважив, що працівники правоохоронних органів зобов'язані неодмінно здійснювати профілактичні заходи. Водночас, на думку дослідника, уповноважені особи можуть виконувати лише ті заходи профілактики, що передбачені їхніми посадовими обов'язками або нормативно-правовими актами [145, с. 191]. Таке твердження ми не можемо повністю підтримати, оскільки окремі працівники правоохоронних органів можуть виконувати функції та завдання, котрі прямо не передбачені їхніми посадовими інструкціями.

Далі нам необхідно визначити детермінанти протиправних діянь, для усунення яких і будуть формулюватися відповідні профілактичні заходи. Наприклад, окрема група дослідників зауважує, що ними є, «…з одного боку, особисті властивості конкретного індивіда (його потреби, погляди, інтереси, ставлення до різних соціальних цінностей і вимог, у тому числі правових), а з іншого – сукупність зовнішніх обставин, які викликають намір і рішення вчинити умисний злочин. Тобто існує взаємодія криміногенних властивостей особи, які склалися під впливом несприятливих умов її формування, із зовнішніми об'єктивними обставинами і ситуаціями» [102, с. 105].

У свою чергу, С. Кулик на основі власного дослідження визначив групи детермінант, що впливають на збільшення проявів окремої категорії протиправних діянь. Зокрема, науковець виокремив такі соціально-економічні детермінанти, як: «…криза інституту сім'ї; значна поляризація населення за матеріальним становищем і рівнем доходу; високий фактичний рівень безробіття; соціально-економічні негаразди, викликані військовим

конфліктом на сході держави та проведенням антитерористичної операції. Комплекс політико-правових детермінант зводиться до таких основних чинників: недостатнє сприяння та підтримка з боку держави громадських організацій, які займаються розвитком спорту, різних напрямів мистецтва та творчості; відсутність дієвої законодавчо визначеної концепції (програми) з розвитку та зміцнення основ моральності в молодшого покоління та підвищення її рівня в суспільстві; невирішеність кримінально-правових проблем конструкцій диспозицій конкретних норм і визначеності санкцій певних злочинів проти моральності» [96, с. 102–113].

З іншого боку, окрема група авторів зазначає, що у випадках, коли на індивідуальному рівні аналізується конкретне кримінальне правопорушення, то це – «…«елементарна частинка» злочинності. Визнається, що і на цьому рівні зберігають свою дію всі фактори, зв’язки та відношення, характерні для філософського і соціологічного рівнів причин злочинності. Тільки тепер вони конкретизуються і переходять у психологічну форму, пояснюючи цілі й мотиви поведінки конкретної людини – злочинця. Причини індивідуального злочину визначаються як неузгодженість поведінки особистості з соціальним середовищем, в основі якої лежать негативні риси, що сформувалися у конкретної людини під впливом певних факторів. При цьому підкреслюється можливість переорієнтації і виправлення такого суб’єкта» [90, с. 21].

Водночас інша група науковців (П. Мельник, Н. Данкович, І. Фрідман) наголошує на тому, що «…причинні зв’язки існують об’єктивно. Тому завдання полягає в тому, щоб правильно вивчити цю причину. Об’єктивний характер причини робить можливим справжнє наукове пізнання, а потім і вплив на виявлені причини з метою усунення шкідливих наслідків. Причина викликає відповідні їй наслідки тільки за певних умов. Причину не можна не відрізняти від умов, оскільки причина встановлює сутність явища і напрям його розвитку, умови сприяють або, навпаки, перешкоджають дії причини, але сутність процесу не визначають. Помилкова оцінка умови як причини явища тягне за собою безплідність спроб усунути шкідливі наслідки,

оскільки усунення однієї з умов при збереженні причини не виключає в принципі настання небажаного результату» [149, с. 16].

А вже щодо дітей, які є потерпілими від певних протиправних діянь, О. Козицька, залежно від умов їхнього життя та виховання, вирізнила такі групи: ті, що проживають і виховуються у повній сім'ї; ті, що проживають і виховуються у неповній сім'ї (сім'я, що складається з матері або батька та дитини); ті, що проживають і виховуються у багатодітній сім'ї; ті, що проживають і виховуються у прийомній сім'ї; ті, що проживають і виховуються у дитячому будинку сімейного типу; ті, що проживають і виховуються у дитячому будинку-інтернаті [70, с. 205].

У свою чергу, Л. Кобилянська слушно зазначила, що «…кіберзлочинність щорічно завдає глобальних економічних збитків, які надзвичайно складно визначити в кількісному виразі. Водночас суб'єкти господарювання та уряди держав недооцінюють реальні виклики та загрози, пов'язані з кіберзлочинами в глобальному вимірі (йдеться про так званий прихований чи «тіньовий» Інтернет, кібертероризм, промисловий шпіонаж, функціонування бот-мереж та вірусних програм). Боротьба з кіберзлочинністю в міжнародному форматі актуалізує необхідність координації дій державного і приватного сектора на основі об'єднання фінансових, технічних, комунікаційних і організаційних ресурсів, обмеження анонімності користувачів у всесвітній Інтернет-мережі, соціальних мережах та під час проведення банкінгових операцій, створення міжнародних підрозділів та структур у боротьбі з кіберзлочинністю з наданням права передачі даних про рух інформації, екстрадицію, допомогу, розробку міжнародних чи транскордонних комунікаційних мереж для відстеження в реальному часі і передачі інформації про кіберзлочини. Втручання в роботу телекомунікаційних систем в Україні потребує вжиття низки заходів протидії, зокрема: зменшення кількості авторизаційних лімітів, розширення використання чіпових карт, застосування сучасного мережевого захисту банківських систем, у тому числі систем додаткового підтвердження

платежів через одноразові паролі та коди. Небезпеку складає одночасне використання браузеру для ігор чи спілкування в соціальних мережах та здійснення Інтернет-банкінгу. Використання ліцензійного програмного забезпечення, новітні системи мережевого захисту фінансових установ та організацій, роз'яснювальна робота серед клієнтів у питаннях збереження конфіденційності інформації та індивідуальних даних сприяє зниженню кількості кіберзлочинів. Існує потреба удосконалення внутрішнього чинного законодавства України шляхом доповнення термінології нормативно-правової бази в сфері кіберзлочинності. Наразі в Україні відсутня єдина державна стратегія з кібербезпеки та цифрового суверенітету, виробництво власних програм та сучасної електронної комп'ютерної техніки, а також єдина національна операційна система обміну інформацією. За відсутності власної технічної, програмної бази країна з низьким рівнем обізнаності, інформаційної безпеки й надалі лишатиметься залежною і вкрай вразливою до глобальних загроз» [62, с. 16–17].

Окрема група дослідників (В. Биков, О. Буров, Н. Дементієвська) надала перелік питань щодо захисту учасників освітньому процесу, а саме: «…1. Призначені для користувача облікові дані є власністю закладу освіти… 2. Потрібно проводити вступні і регулярні заняття для працівників та учнів, спрямовані на підвищення рівня знань з інформаційної безпеки. 3. Обов'язковими мають бути регламент з безпеки, а також інструкції, до яких користувач завжди міг би мати доступ… 4. Комп'ютери користувачів завжди повинні мати актуальне антивірусне програмне забезпечення. 5. У корпоративній мережі закладу освіти або об'єднання освітніх закладів необхідно використовувати системи виявлення атак та запобігання таким атакам. Потрібно також використовувати системи запобігання витоку конфіденційної інформації. Усе це дасть змогу знизити ризик виникнення фішингових атак. 6. Потрібно бути пильним щодо ресурсу, який запитує конфіденційні дані. 7. Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса

відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд» [8].

На основі вищенаведених тверджень нами було вирізнено причини та умови, що впливають на вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, як-от:

1) недосконалість діючих нормативно-правових актів;

2) наявність нормативно-правових колізій стосовно оптимальної реалізації е-банкінгу;

3) прогалини, що наявні у кримінальному законодавстві;

4) суперечливість судової практики щодо кримінальних правопорушень, учинених у кіберпросторі;

5) транснаціональний характер протиправних дій;

6) хакерські атаки на сайти, де здійснюються операції е-банкінгу;

7) допомога протиправним діям із боку працівників банків, інтернет-провайдерів, операторів мобільного зв’язку.

Стосовно конкретних профілактичних заходів, що їх мають реалізовувати уповноважені особи правоохоронних органів при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу, звернемося до деяких досліджень науковців. Так, М. Єфімов та К. Чаплинський виокремили з-поміж них такі: «…здійснення виховного впливу підрозділами на неповнолітніх і малолітніх осіб шляхом пропаганди ненасильства та дотримання суспільної моралі; здійснення підрозділами профілактичного впливу на громадян; участь працівників підрозділів у тематичних передачах, круглих столах, ток-шоу, що висвітлюють проблеми суспільства у сфері порушення норм моралі; організація дискусій у друкованих ЗМІ, присвячених актуальним питанням моралі» [38, с. 276].

Також досить цікавою є позиція А. Микитчик, який відмітив, що «…міжнародне співробітництво є ключовим моментом в ліквідації правового вакууму, який існує між розвитком інформаційних технологій і реагуванням на них законодавцем. Технічний підхід передбачає запобігання

кіберзлочинам за рахунок реалізації заходів технічного характеру, що забезпечують безпеку в інформаційній сфері, а також формування матеріально-технічної бази підрозділів по боротьбі з кіберзлочинністю, виходячи з принципу «найсучасніша техніка». Організаційний підхід має на меті розробку і запровадження в практику удосконалених організаційно профілактичних заходів. Перш за все слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій і перейти до активної розробки інформаційної безпеки на випередження. Необхідно об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян. Запобігання кіберзлочинності має включати в себе заходи віктимологічної профілактики – підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації. Актуальними є поглиблені виктимологічні кримінологічні дослідження кіберзлочинності, спрямовані на виявлення об'єктивних закономірностей, детермінант кіберзлочинності, характеристик окремих типів особистості кіберзлочинців, а також різних аспектів забезпечення кібербезпеки» [123, с. 137–138].

А вже О. Борідько та А. Гаркуша наголошували, що діяльність уповноваженої особи під час здійснення кримінального провадження має суворо цілеспрямований характер. Крім того, автори вказували, що зазначена особа повинна встановити дії осіб і недоліки, що мають місце в роботі установ, підприємств, які сприяли вчиненню протиправного діяння. Наведені чинники, на думку дослідників, мають обумовлювати найменування акта, в якому відображаються рішення про усунення вказаних обставин. Як підсумок науковці зауважують, що є правильним називати процесуальний акт, за допомогою якого уповноважена особа реагує на причини і умови, що сприяли вчиненню кримінального правопорушення, так: «Подання про недоліки в роботі установи (підприємства, організації)», «Подання про невиконання обов'язків (конкретною особою)» [18, с. 71].

Зі свого боку, О. Антонюк вирізнив такі заходи профілактичної діяльності підрозділів правоохоронних органів: «…а) своєчасне реагування на заяви та повідомлення стосовно вчинення протиправних діянь, затримання підозрюваних з огляду наявності законних підстав, вибір відносно останніх відповідних запобіжних заходів; б) залучення правоохоронців до проведення ток-шоу, тематичних передач, круглих столів, на яких розглядаються випадки порушення громадського порядку та умови його забезпечення; в) застосовування окремих процесуальних дій з метою здійснення криміналістичної профілактики (допиту, пред'явлення підозри); г) реалізація профілактичного впливу на окремі категорії осіб шляхом пропаганди ненасильства та дотримання громадського порядку; д) опрацювання та аналіз судово-слідчої практики для виявлення та усунення умов й причин, що сприяли вчиненню протиправних діянь; е) організація диспутів у різноманітних ЗМІ з актуальних питань забезпечення громадського порядку; є) застосовування наявних можливостей техніко-криміналістичного забезпечення для здійснення криміналістичної профілактики» [1, с. 277].

У свою чергу, А. Жилін із-поміж профілактичних заходів, котрі варто реалізувати уповноваженим особам правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів, виокремив такі, як: «…повідомлення громадянам через засоби масової інформації про юридичну відповідальність за шахрайську діяльність в сфері використання банківських електронних платежів; виявлення осіб, схильних до антисуспільної поведінки в сфері комп'ютерної діяльності (хакери, фішери) та подальша їх постановка на облік у підрозділах кіберполіції; інформування населення через засоби масової інформації, месенджери та соціальні мережі про випадки вчинення шахрайських дій у сфері використання банківських електронних платежів (фішинг, кардинг, сніфферінг); попередження повторних (рецидивних) проявів шахрайства досліджуваного виду шляхом максимально повного викриття усіх осіб, задіяних у вчиненні конкретного протиправного діяння з подальшим

внесенням їх у відповідний облік» [39, с. 214].

На основі опрацювання судово-слідчої практики та вищенаведених позицій дослідників нами було вирізнено профілактичні заходи, що можуть проводитись уповноваженими особами різних підрозділів правоохоронних органів стосовно усунення причин та умов вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, як-от:

1) повідомлення громадян за допомогою засобів масової інформації про юридичну відповідальність за учинені протиправні дії;

2) встановлення осіб, схильних до антисуспільної поведінки у сфері використання ЕОТ, а також їх подальше занесення до обліку в підрозділах кіберполіції;

3) участь працівників кіберполіції у тематичних передачах, круглих столах, ток-шоу, де висвітлюються питання запобігання протиправним діям у кіберпросторі;

4) вивчення матеріалів кримінальних проваджень для з’ясування та усунення умов і причин, що сприяли вчиненню протиправних діянь;

5) інформування громадян у соціальних мережах, ЗМІ, месенджерах щодо фактів учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу (фішингу, кардингу, спамінгу).

Також нами наведено деякі факти стосовно аналізу технічних та програмних можливостей ЕОТ, а також специфіки діяльності мережі Інтернет. Зокрема встановлено, що вказане може свідчити як про злочинні дії, так і про попередження їхніх проявів.

Крім того, опрацьовано модель прояву властивостей кіберзагроз у транзакціях користувачів е-банкінгу. Найбільш слушною вважаємо думку Ю. Чаплінської, яка зауважила, що «…двохетапна аутентифікація важлива не лише у воєнний, а й у мирний час, оскільки завдяки цій процедурі користувачі різних видів послуг можуть убезпечити себе від кіберзлочинності. Отже, двохетапна аутентифікація – це підтвердження входу в інтернет-банкінг, різноманітні акаунт, особисті кабінети за

допомогою телефона (додаткового дзвінка на ваш номер або СМС із кодом-підтвердженням). Якщо ця функція увімкнена, то це серйозно ускладнює, а інколи й унеможливлює для кібезлочинців отримання доступу до персональних даних користувача, оскільки для входу потрібне додаткове підтвердження через доступ до телефонного номера користувача. Більшість банків без цієї функції взагалі не працюють. Двохетапну аутентифікацію необхідно увімкнути і в Google-акаунтах. Якщо ви користуєтеся телефоном на системі Android, то Google-акаунт – це і є ваш телефон з усіма даними на ньому» [195, с. 26].

Також нами було встановлено, що однією з головних причин неефективності заходів із запобігання кримінальним правопорушенням, пов'язаним із використанням е-банкінгу, залишається низький рівень обізнаності слідчих та працівників оперативних підрозділів Національної поліції України щодо типових злочинних схем під час здійснення незаконних банківських операцій та напрямів збирання електронних доказів, встановлення правопорушників за цифровою слідовою картиною, особливостей документування злочинних дій у кіберпросторі та ін.

Підсумовуючи, відмітимо, що запобігання протиправним діянням із кожним роком стає все більш важливим напрямом діяльності всіх підрозділів правоохоронних органів. Надано авторське визначення профілактики протиправних діянь як спеціального різновиду правоохоронної діяльності, що складається з конкретної сукупності певних дій та заходів, котрі реалізують працівники правоохоронних органів (слідчі, дізнавачі, детективи, прокурори), та має метою усунення причин і умов скоєння окремих категорій кримінальних правопорушень. Вирізнено профілактичні заходи, котрі можуть проводитись уповноваженими особами різних підрозділів правоохоронних органів стосовно усунення причин та умов вчинення кримінальних правопорушень.

Висновки до розділу 2

Під час аналізу особливостей початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу, типових слідчих ситуацій, а також форм взаємодії окремих підрозділів поліції та напрямів реалізації профілактичних заходів у досліджуваній категорії кримінальних проваджень було сформульовано такі висновки:

1. Визначено, що початковий етап розслідування характеризується такими етапами, як: отримання повідомлення про вчинене правопорушення, аналіз початкової інформації та внесення відомостей до ЄРДР у разі її підтвердження. Наведений алгоритм дій зумовлює стислі строки реалізації первинних заходів для встановлення особи злочинця, збирання доказової бази та формування кола обставин, що підлягають встановленню. Важливого значення набуває невідкладність проведення огляду місця події. Наголошено на труднощах, які виникають на початковому етапі розслідування, що зумовлено відсутністю злочинця на місці події.

2. На основі аналізу матеріалів кримінальних проваджень з’ясовано, що підставою для внесення даних до Єдиного реєстру досудових розслідувань за фактом учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, стали початкові дані, що надійшли до правоохоронних органів із таких джерел, як: а) заяви, листи й повідомлення, що надійшли від потерпілих, – 79 %; б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене кримінальне правопорушення або були свідками його скоєння, – 8 %; в) повідомлення працівників установ, підприємств та організацій – 3 %; г) матеріали досудового розслідування, виділені з інших кримінальних проваджень – 4%; д) матеріали, одержані в ході проведення НСРД та розшукових заходів – 7 %.

3. Надано рекомендації стосовно оцінки первинної інформації, що надходить до правоохоронних органів. Вирізнено типові слідчі ситуації, що

формуються на початковому етапі розслідування протиправного діяння, а також визначено відповідні тактичні завдання, котрі необхідно вирішити у кожній із них. Окреслено тактичні помилки, що їх припускаються слідчі, які розпочали розслідування: прорахунки у діагностуванні злочинної події та визначенні напрямів розслідування – 84 %, порушення процесуального порядку проведення СРД – 62 %, проведення невідкладних слідчих (розшукових) дій без участі спеціаліста – 57 %, ігнорування встановлення низки важливих обставин – 37 %, «поверхневий» характер невідкладних слідчих (розшукових) дій (огляд, обшук) – 29 % та ін.

4. На основі наукових розробок дослідників (М. Погорецький, К. Чаплинський, Ю. Чорноус, О. Юхно) з'ясовано, що правильно спланована й організована взаємодія різних підрозділів Національної поліції України забезпечить отримання достатньої доказової інформації для найбільш ефективного проведення процесуальних дій та розшукових заходів. Взаємодію сформульовано як спільну й взаємообумовлену діяльність окремих підрозділів Національної поліції України, котру визначено нормативно-правовою базою та погоджено за місцем, часом і єдиною метою функціонування окремих підрозділів, що виявляється в оптимальному проведенні спільних організаційно-тактичних заходів для запобігання та розслідування протиправних посягань. Така діяльність здійснюється під єдиним керівництвом, що зводиться до проведення усіх слідчих (розшукових) дій, НСРД та розшукових заходів у чіткій співпраці та координації з метою найбільш швидкого і ефективного досягнення та вирішення завдань конкретного кримінального провадження.

5. З'ясовано особливості взаємодії уповноважених осіб (слідчих, дізнавачів, прокурорів, детективів) з іншими працівниками правоохоронних органів, а також різних установ, підприємств та організацій, громадськістю тощо. Особливу увагу приділено найбільш розповсюдженим формам взаємодії підрозділів Національної поліції України, особливо з підрозділами Департаменту кіберполіції, – організаційній та процесуальній.

6. Наголошено на важливості використання обміну інформацією як однієї з найбільш ефективних форм взаємодії, особливо в умовах запровадженого воєнного стану. Така інформація може стосуватися наступних обставин: а) ознак злочинного діяння, пов'язаного з використанням е-банкінгу (яке вчинене або знаходиться на етапі підготовки); б) структури ОГ та ЗО, що здійснюють тривалу злочинну діяльність в економічній сфері; в) характерних ознак злочинців (хакерів, спамерів, фішерів, фрікерів, кіберсквотерів, лідерів ОЗГ та їхніх членів), які здійснюють протиправну діяльність.

7. Наголошено, що ефективна протидія злочинним проявам у сфері використання банківських електронних платежів вимагає від правоохоронних органів не тільки збирання доказової інформації, але й забезпечення певної профілактичної функції. Доведено, що одним із основних напрямів організації розслідування кримінальних правопорушень є вжиття ефективних заходів щодо їх запобігання.

8. Окреслено основні напрями профілактичної діяльності працівників правоохоронних органів щодо виявлення й усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а також відповідні заходи, що спрямовані на своєчасне їх попередження та усунення. Профілактику протиправних діянь визначено як спеціальний різновид правоохоронної діяльності, що складається з конкретної сукупності певних дій та заходів, котрі реалізують працівники правоохоронних органів (слідчі, дізнавачі, детективи, прокурори), та має метою усунення причин і умов скоєння окремих категорій кримінальних правопорушень.

9. Вирізнено причини та умови, що впливають на вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от: 1) недосконаліть діючих нормативно-правових актів; 2) наявність нормативно-правових колізій стосовно оптимальної реалізації е-банкінгу; 3) прогалини, що наявні у кримінальному законодавстві; 4) суперечливість

судової практики щодо кримінальних правопорушень, учинених у кіберпросторі; 5) транснаціональний характер протиправних дій; 6) хакерські атаки на сайти, де здійснюються операції е-банкінгу; 7) допомога протиправним діям із боку працівників банків, інтернет-провайдерів, операторів мобільного зв'язку. Запропоновано заходи профілактики, що можуть здійснюватися уповноваженими особами у кримінальних провадженнях для попередження кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

10. Наведено деякі факти стосовно аналізу технічних та програмних можливостей ЕОТ, а також специфіки діяльності мережі Інтернет. Зокрема встановлено, що вказане може свідчити як про злочинні дії, так і про попередження їхніх проявів. Опрацьовано модель прояву властивостей кіберзагроз у транзакціях користувачів е-банкінгу. Підтримано позицію щодо внесення в чинний Кримінальний процесуальний кодекс України норми, в якій буде зазначено про обов'язок працівників правоохоронних органів (слідчих, дізнавачів, детективів, прокурорів) забезпечувати усунення причин та умов, що сприяли вчиненню протиправних діянь. Оскільки вказаний обов'язок забезпечить постійну реалізацію відповідних профілактичних заходів.

Основні результати розділу опубліковано у працях [113; 118; 119].

РОЗДІЛ 3
КОМПЛЕКСИ ТАКТИЧНИХ ОПЕРАЦІЙ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ Е-БАНКІНГУ

3.1. Тактичні операції щодо збирання первинної інформації про обставини події та виявлення ознак кримінального правопорушення

Тактичні операції – це загальноприйнятий засіб криміналістичної тактики нарівні з тактичним прийомом, тактичною рекомендацією і тактичним рішенням. Більшість учених-криміналістів однозначно підтримує зазначену позицію. Під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, значення вказаної наукової категорії не втрачає своєї важливості. Оскільки під час її реалізації можна отримати максимальну кількість доказової інформації для доведення вини правопорушника. З огляду на зазначене дослідження тактичних операцій у межах нашої роботи вважаємо беззаперечно важливим [121, с. 178].

Для початку наведемо твердження А. Жиліна, який зауважував, що «на часі в криміналістиці існує така наукова категорія, як «тактичні операції». З іншого боку, в загальній теорії методики розслідування кримінальних правопорушень вказаний інструмент майже не зустрічається. В свою чергу, ми вважаємо його найбільш оптимальним для кримінальних проваджень щодо випадків вчинення шахрайства у сфері використання банківських електронних платежів. Оскільки визначені діяння після внесення відомостей в ЄРДР одразу потребують швидкого проведення відповідних НСРД та інших процесуальних заходів. Адже шахраї в досліджуваній категорії кримінальних проваджень мають високий інтелектуальний розвиток та комп'ютерну грамотність. Тому будь-яке зволікання в процесі реалізації вказаних дій може призвести до знищення важливої доказової інформації

(віртуальної, матеріальної чи ідеальної). В той час як реалізація відповідних тактичних операцій максимально убезпечить працівників правоохоронних органів від зазначених негативних наслідків» [42, с. 134].

Крім того, вважаємо доречною думку А. Чорного, який відмічав, що «…на практиці криміналістичні комплекси у вигляді тактичних операцій використовуються ще досить рідко, слідчі замість них віддають перевагу послідовному проведенню окремих слідчих дій, які за своїм призначенням і часом проведення нерідко порушують логіку пошуку доказів, які підтверджують висунуту версію. Послідовність проведення окремих слідчих (розшукових) дій нерідко спричиняє втрату інформації, створює часовий потенціал для злочинців, використовуваний для приховування або знищення доказів, залякування свідків, придумування неправдивих алібі тощо. У цьому аспекті проведення тактичних операцій сприяє не тільки швидкості одержання необхідної інформації, але й усуненню перешкод, які створюються для її одержання» [202, с. 238].

З огляду на вищенаведену роботу А. Жиліна, а також на праці С. Кузьменка [93], О. Мусієнка [127], Н. Павлової [137], А. Рейнгольда [155] ми пропонуємо підхід до розгляду методики розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу, крізь призму проведення комплексів тактичних операцій.

Що стосується безпосередньо формулювання тактичної операції, то, наприклад, Р. Степанюк писав про неї таке: «…повинна розглядатись як комплекс слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів, спрямованих на виконання проміжного завдання розслідування у певній слідчій ситуації. У свою чергу, типові тактичні операції являють собою визначені на підставі узагальнення слідчої практики алгоритми дій слідчого, спрямовані на вирішення проміжних завдань, що виникають на певних етапах розслідування у типових слідчих ситуаціях. Для формування окремих методик розслідування злочинів, вчинених у бюджетній сфері України, найбільше значення має диференціація типових тактичних

операцій стосовно рівнів методик (універсальні, загальні й окремі тактичні операції) і проміжних завдань розслідування, у зв'язку з чим можуть бути диференційовані загальні тактичні операції, які конкретизуються в методиках розслідування нижчого рівня» [183, с. 370]. А вже К. Чередник вказувала на те, що «…процес розслідування стає найбільш оптимальним, якщо проводиться не одна, а кілька тактичних операцій, що дозволяють не тільки успішно вирішити проміжні завдання, а й максимально наблизитися до досягнення кінцевої мети розслідування. Зміст і спрямованість тактичної операції обумовлені, по-перше, слідчою ситуацією, а по-друге, видовими особливостями розслідуваного злочину» [197, с. 134].

Водночас С. Здоровко у своєму дослідженні запропонував визначення тактичної операції «…як системи однойменних або різнойменних процесуальних або непроцесуальних дій і заходів (слідчих, оперативно-розшукових, організаційних), які спрямовані на вирішення проміжного завдання розслідування, об'єднані єдиним планом і єдиним задумом, характеризуються вибірковістю і ситуаційною обумовленістю та виконуються правомочними посадовими особами під керівництвом слідчого» [52, с. 4].

У свою чергу, М. Салтевський наголошує на тому, що зазначена наукова категорія – це засіб діяльності уповноваженої особи, що використовується для вирішення тактичних завдань, які виникають при розкритті, розслідуванні і попередженні кримінальних правопорушень [161, с. 79]. Зі свого боку, К. Латиш з огляду на стале поєднання тактичних завдань і тактичних операцій зауважив, що вони повинні складатися в таку трьохчленну структуру, компонентами якої будуть тактичні проміжні (локальні) завдання під час розслідування: пізнавальні, діагностичні та пошукові тактичні завдання, розв'язанню яких слугують конкретні тактичні операції [103, с. 115].

Цікавою є думка П. Біленчука та В. Перкіна, які формулюють досліджувану наукову категорію як «…комплекс слідчих дій, оперативно-

розшукових, організаційно-технічних та інших заходів, спрямованих на досягнення конкретної мети в ході розслідування злочинів» [11, с. 16].

Також досить слушно С. Шевчук акцентував увагу на тому, що «…після прийняття рішення про проведення певної тактичної операції відбувається побудова моделі цієї операції і створення програми її реалізації. До програми має бути включено системний перелік методичних рекомендацій та конкретних дій щодо вибору засобів розв'язання сформульованих тактичних завдань, визначення послідовності їх застосування, з урахуванням часу, місця і початку операції. Поряд із цим до загальної моделі програми тактичної операції можуть входити моделі дій кожного з її учасників або моделі здійснення тієї чи іншої слідчої дії, що входить до складу тактичної операції» [209].

Крім того, окрема група авторів (В. Кузьмічов, Г. Прокопенко) до елементів тактичної операції, крім слідчих (розшукових) дій та оперативно-розшукових заходів, занесла й такі, як: «…перевірочні дії відповідно до ст. 97 КПК України; організаційно-технічні заходи; заходи щодо використання засобів масової інформації; заходи щодо використання допомоги громадськості; заходи виховного впливу слідчого на осіб, залучених до сфери кримінального судочинства (передбачені нормативними актами МВС України); заходи в межах охорони громадського порядку (проведені в зв'язку з іншими заходами тактичної операції)» [95, с. 197].

Підбиваючи підсумки, надамо авторське визначення тактичної операції як комплексу процесуальних дій та заходів, котрі направлені на розв'язання певного тактичного завдання, що відіграє важливу роль під час розслідування різних категорій кримінальних правопорушень.

Із приводу тактичних завдань, що потребують вирішення під час проведення тактичних операцій, зокрема, С. Здоровко вказує на те, що «…тактичне завдання – це певна проблема, яка потребує свого вирішення в процесі розслідування, має відокремлений характер різного ступеня, передбачає використання різноманітних тактичних засобів (тактичних

операцій, слідчих дій, оперативно-розшукових заходів, тактичних комбінацій, тактичних або інших прийомів). Типізація завдань дозволить встановити напрямок розслідування, окреслити коло проблем, що потребують свого вирішення, встановити типові засоби їх вирішення» [50, с. 12]. Ми повністю поділяємо зазначену позицію та наведемо окремі позиції дослідників з цього питання.

Наприклад, О. Курман наголошував на тому, що в ситуації встановлення ознак шахрайства з фінансовими ресурсами потрібно вирішити низку завдань, а саме встановити: «…1) обставини створення фірми-позичальника (законність заснування, справжність установчо-реєстраційних документів); 2) дійсність фінансово-господарських документів; 3) достовірність наданих гарантійних документів; 4) обґрунтованість кредитного проекту (техніко-економічного обґрунтування); 5) законність одержання кредиту або надання пільг з оподаткування; 6) цілі витрат одержаних коштів; 7) осіб, причетних до вчинення злочину і ступінь їхньої вини; 5) майно (нерухоме і рухоме), грошові кошти, необхідні для відшкодування завданих збитків і вжити заходи для їх збереження» [100, с. 147].

Також досить цікавим є твердження С. Кузьменка, котрий виокремлює завдання, пов’язані зі збиранням відомостей під час розслідування шахрайства, пов’язаного з інвестуванням коштів у будівництво об’єктів нерухомості, як-от: «…1) обставини, що передували вчиненню шахрайства; 2) місця, де здійснювалися шахрайські дії; 3) час вчинення шахрайських дій та тривалість їх у часі; 4) способи шахрайських дій щодо заволодіння обманним шляхом грошима інвесторів; 5) кількість епізодів злочинної діяльності та наявність в діях злочинців ознак інших супутніх злочинів; 6) кількість потерпілих-інвесторів, які постраждали внаслідок дій шахраїв; 7) компанію забудовника; 8) осіб, які брали участь у вчиненні шахрайства, їх кількість та роль кожного; 9) осіб, які можуть надати криміналістично-значиму інформацію про обставин вчинення шахрайства, та осіб, які до цього

причетні; 10) збирання іншої інформації щодо події та джерел криміналістично значимої інформації» [94, с. 54].

Зі свого боку, М. Костенко з-поміж тактичних завдань, що потребують вирішення під час розслідування кримінальних правопорушень, вчинених організованими злочинними угрупованнями, виокремив такі: «…1) тактичне завдання щодо встановлення кількісного складу групи осіб; 2) тактичне завдання щодо встановлення стійкості зв'язків між членами групи; 3) тактичне завдання щодо встановлення наявності єдиного і відомого всім учасникам групи плану злочинної діяльності; 4) тактичне завдання щодо встановлення розподілу функцій учасників групи, спрямованих на реалізацію плану злочинної діяльності» [78, с. 149–150].

Зважаючи на зазначене, вважаємо за потребу навести тезу С. Бренер, яка зауважувала, що найдосконаліші кіберпереслідувачі використовують програми для надсилання повідомлень через регулярні або випадкові проміжки часу, не перебуваючи фізично біля комп'ютерного термінала. Також авторка навела приклад: правоохоронні органи Каліфорнії вказували, що стикалися з ситуаціями, коли жертва неодноразово отримувала на своїх пейджерах повідомлення «187» – розділ Кримінального кодексу Каліфорнії про вбивство. Крім того, дослідниця відмітила, що кіберпереслідувач може змусити інших користувачів Інтернету переслідувати або погрожувати жертві, використовуючи дошки оголошень або чат-кімнати. Зокрема, сталкер може опублікувати суперечливе або привабливе повідомлення на дошці під іменем, номером телефону або адресою електронної пошти жертви, що призведе до наступних відповідей, котрі будуть надіслані жертві. Кожне повідомлення – чи від самого кіберпереслідувача, чи від інших – матиме очікуваний вплив на жертву, але зусилля кіберпереслідувача мінімальні, а відсутність прямого контакту між кіберпереслідувачем і жертвою може ускладнити правоохоронним органам ідентифікацію, встановити місцезнаходження та затримати порушника [216].

У свою чергу, А. Рейнгольд, формулюючи тактичні завдання під час

розслідування шахрайства в інтернет-комерції, вказав, що серед них існує перелік завдань, що направлені на: «…виявлення шахрайських операцій шляхом перевірки за різними фільтрами; перевірку історії проведених транзакцій; встановлення місцезнаходження точки доступу до інтернету та провайдера, який сприяв доступу до мережі інтернет; отримання інформації, що міститься у поштовій скринці; встановлення справжності чи фіктивності інтернет-сайтів; встановлення шахрайського умислу та виключення форсмажорних обставин, що не надали можливість виконати договірні зобов'язання тощо» [156, с. 179].

А вже К. Чередник зауважувала, що одним із основних тактичних завдань також є комплекс дій, спрямований на: встановлення свідків, які можуть надати інформацію про подію, встановлення осіб, які мають стосунок до вчинення зазначеного шахрайства, з'ясування взаємовідносин цих осіб та характеру їхньої участі у вчиненому злочині. З огляду на зазначене авторка дійшла висновку, що для вирішення вказаних завдань варто проводити такі тактичні операції, як: «розшук», «затримання», «співучасники», «встановлення свідків», «сукупність злочинів», «встановлення ознак організованості» [198, с. 180].

На основі вищевикладеного вважаємо за необхідне виокремити завдання, котрі потрібно вирішувати для здійснення тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от:

1) обставини, що передували вчиненню протиправних дій;

2) способи вчинення протиправних дій (фішинг, застосування шпигунських програм, спам-ботів);

3) електронно-обчислювальна техніка, що використовувалася для здійснення протиправних дій;

4) час і тривалість злочинних дій;

5) учасники, їхня кількість і роль кожного в учиненні протиправних дій;

6) загальна кількість потерпілих та їх характеристика.

Залежно від проміжних (локальних) завдань розслідування кримінальних правопорушень С. Здоровко виокремлює такі тактичні операції, як: «…тактична операція «Встановлення злочинця»; тактична операція «Документ»; тактична операція «Атрибуція трупа»; тактична операція «Виявлення зв'язків організованої злочинної групи»; тактична операція «Допущення обшуку з негативним результатом»; тактична операція «Затримання по гарячих слідах»; тактична операція «Захист доказів»; тактична операція «Встановлення знарядь злочину»; тактична операція «Відшкодування матеріального збитку»; тактична операція «Розшук злочинця» та ін.» [51, с. 35].

У свою чергу, А. Рейнгольд, з огляду на вищезазначені завдання розслідування, окреслив такі «…типові тактичні операції: "Фальшивий сайт", "Незаконна транзакція", "Встановлення IP-адреси", "Ідентифікація особи у віртуальному просторі", "Встановлення умислу", "Організація затримання шахрая, який діяв в мережі інтернет"» [155, с. 15].

Також вважаємо вельми докладним перелік тактичних операцій, наведений О. Курманом, а саме: «Документ», «Співучасники», «Позичальник», «Кредитор», «Розшук злочинця, що переховується», «Забезпечення відшкодування матеріальних збитків» [99, с. 13].

Крім того, В. Шевчук надав досить повний перелік тактичних операцій, що реалізуються під час розслідування кримінальних правопорушень, зокрема: 1) «Встановлення характеру події злочину»; 2) «Встановлення місця і часу вчинення злочину»; 3) «Встановлення способу вчинення злочину»; 4) «Встановлення предмету злочинного посягання»; 5) «Встановлення мотивів вчинення злочину»; 6) «Встановлення особи злочинця»; 7) «Встановлення особи потерпілого (жертви)»; 8) «Встановлення провокуючої поведінки жертви»; 9) «Перевірка зв'язків потерпілого»; 10) «Встановлення співучасників злочину»; 11) «Затримання злочинця на місці злочину»; 12) «Розшук особи, яка зникла з місця події і переховується

від слідства»; 13) «Перевірка алібі підозрюваного»; 14) «Встановлення свідків»; 15) «Перевірка обмови»; 16) «Перевірка самообмови»; 17) «Нейтралізація протидії розслідуванню з боку зацікавлених осіб»; 18) «Вивчення особи підозрюваного»; 19) «Усунення негативного впливу з боку підозрюваного; 20) «Захист доказів»; 21) «Захист потерпілих»; 22) «Захист свідків» [208, с. 138].

На основі вищенаведених думок науковців сформулюємо власний перелік тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от:

– «Встановлення характеру події кримінального правопорушення»;

– «З'ясування місця та часу вчинення протиправного діяння»;

– «Встановлення способу вчинення протиправного діяння (фішинг, застосування шпигунських програм, спам-ботів)»;

– «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання».

З приводу процесуальних дій, котрі можуть входити до вищезазначених тактичних операцій, розглянемо різні праці науковців. Зокрема, К. Чередник наводить процесуальні дії, що можуть входити до тактичних операцій, спрямованих на встановлення ознак організованості, а саме: «…допити свідків, потерпілих, співучасників; пред'явлення для впізнання предметів, документів, осіб; проведення НСРД, спрямованих на спостереження за особою, річчю або місцем, зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем (спостерігання за членами групи, які знаходяться на волі, та прослуховування їхніх розмов); виконання спеціального завдання щодо участі в ЗУ особи, яка на конфіденційній основі співпрацює з органами досудового розслідування (впровадження в групу); контроль за вчиненням злочину; тимчасовий доступ до речей та документів та провадження одночасних обшуків; огляд вилучених предметів та документів; призначення

судових експертиз (почеркознавчої, технічної експертизи документів, комп'ютерної техніки та програмних продуктів, економічної, судово-психологічної тощо); проведення ОРЗ, спрямованих на отримання інформації про співучасників та осіб, які могли сприяти вчиненню злочину; ОРЗ, спрямовані на встановлення місцезнаходження осіб, які переховуються від слідства та суду; проведення СРД, ОРЗ, спрямованих на розшук активів та накладення на них арешту тощо» [196, с. 12].

На основі узагальнення судово-слідчої практики запропоновано перелік слідчих (розшукових) дій, НСРД та інших процесуальних заходів, необхідних для ефективного здійснення тактичних операцій у кримінальному провадженні: огляд місця події, огляд ЕОТ, допит потерпілого, зняття інформації з електронних інформаційних систем або її частини, встановлення місцезнаходження радіоелектронного засобу, допит підозрюваного, обшук, пред'явлення для впізнання, обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерпол, Європол) стосовно реагування на кіберзлочини. Крім того, з-поміж них виокремлено та охарактеризовано найбільш важливі, а саме огляд ЕОТ та допит підозрюваного.

Щодо огляду ЕОТ слід навести позицію І. Коновалової, яка зазначила: «…кожне замовлення, розміщене в інтернет-магазині, надходить з унікальної загальнодоступної IP-адреси. За IP-адресою, зазвичай, можна визначити місто чи регіон світу, де споживач здійснює покупку. Якщо це місто чи регіон не збігається з адресую кредитної картки, яка використовується, це може означати загрозу шахрайства. Використання програм для боротьби з шахрайством. Коли справа доходить до виявлення та запобігання шахрайству в електронній торгівлі, існує безліч програмних рішень, які відповідають різним потребам та бюджету. Прості програми боротьби з шахрайством виконують специфічну функцію. Зазвичай, вони інтегровані в онлайн-кошики та платформи електронної комерції. Ці інструменти використовують алгоритми машинного навчання для виявлення шахрайських транзакцій за

допомогою геолокації IP, перевірки адрес електронної пошти, проведення відбитків пальців пристрою та перевірки адрес. Програми для боротьби з шахрайством середнього рівня пропонують більш широкий спектр функцій, включаючи гарантії повернення платежів, автоматичне відхилення замовлень із високим ризиком, захист від нових шахрайств з обліковими записами та захист від поглинання облікового запису. Програми найвищого рівня захисту виконують всі ті ж функції, що й вищезазначені програми, а також пропонують аутсорсингове управління справами, роботу з великими продавцями, управління шахрайством із лояльністю, захист від зловживання політикою, автоматичне прийняття рішень та ручний перегляд підозрілих транзакцій, гарантуючи, що жодне хороше замовлення не буде помилково відхилено програмним забезпеченням. Відповідні програми при оплаті автоматизують перевірки на шахрайство, здійснюють блокування підозрілих пристроїв, скасування шахрайських замовлень та багато іншого» [74, с. 223]. Тобто дослідниця вказала на важливість огляду окремих складових ЕОТ та надала їм характеристики.

У свою чергу, окрема група науковців (П. Біленчук, Д. Біленчук, В. Міщенко, О. Мотлях), зауважила, що «…огляд комп'ютерної техніки дозволяє з'ясувати ряд відомостей про способи скоєння шахраєм протиправної дії та їх вірогідні мотиви і мету. В окремих випадках бажано, щоб підозрюваний був присутній при огляді його комп'ютера, оскільки саме він може надати найважливішу інформацію про особливості функціонування комп'ютерної системи, таку як: 1) паролі, коди доступу; 2) перелік інстальованих комп'ютерних програм (програм, які є у комп'ютері); 3) місцезнаходження окремої інформації на машинному носії (окремих директорій, у тому числі прихованих)» [10, с. 66–67].

А вже І. Коваленко констатував, що окрему увагу «…доцільно приділити питанням підготовки комп'ютерної техніки, яка використовується для зчитування і видалення комп'ютерної інформації. Для вирішення цього питання хотілося б запропонувати комплект

науково-технічних засобів, до складу якого включити: Note Book (повинен бути оснащений максимальним набором контактів (1xLPT (EPP / ECP), 1xCOM, 1xPS / 2,1xFIR (інфрачервоний порт), 1xMonitor port, 4xUSB 2.0, 1xFireWire, 1xRJ45 (LAN), 1xRJ11 (факс / модем), 1xTV-out (S-video), 1xVideo-in, 1x аудіо вихід, 1x вхід для мікрофона, 1xS / PDIF-out, мережевий роз'їм і т.д.) з можливістю підключення якнайбільшої кількості комп'ютерних засобів (хардварного обладнання (зовнішніх модемів), PCMCIA BIOS-ом і DOS-ом (мережева карта), миша і клавіатура, принтер і сканер, зовнішній привід, медіа-фото, флеш-драйв тощо); спеціальні програмні засоби (наприклад, програмне забезпечення Vogon International, яке дозволяє створювати точні дублікати або образи жорстких дисків; Gen Tree – проводить складні контекстні пошуки і вивчення графічних і інших об'єктів, система Ilook – забезпечує зняття і стиснення копії (образу) змісту досліджуваного носія для подальшого компактного зберігання і прямого доступу до даних досліджуваного носія і т.п.) для всебічного дослідження і аналізу інформації на місці проведення слідчої дії; кабелі, шнури, перехідники для підключення до ЕОМ (електронно-обчислювальні машини) додаткових пристроїв; набір носіїв інформації: жорсткий диск (вінчестер) з великою місткістю інформації, компакт-диски, флешкарти; набір електромонтажних інструментів; набір вимірювальних приладів; технічна бібліотека в електронному вигляді (може бути корисною для пошуку інформації, щодо якої у фахівця виникають певні сумніви). На відміну від інших, цей набір спеціалізованих засобів повинен постійно модернізуватися, поповнюватися новими програмами та даними, а технічні засоби – оновлюватися» [65, с. 119].

Крім того, Д. Птушкін акцентує увагу 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. Крім того, на флеш-карті мобільного телефону також може зберігатися значна кількість інформації про контакти, зв’язки тощо. Тому така інформація, безсумнівно, становить інтерес для слідства та спрямовує правоохоронні органи у вірному напрямку» [151, с. 100].

Підсумовуючи, зазначимо, що огляд ЕОТ є важливим заходом більшості тактичних операцій, що застосовуються під час розслідування кримінальних правопорушень, вчинених із використанням е-банкінгу. Для ефективного проведення вказаної СРД необхідно ретельно здійснити підготовчі заходи, а також фіксацію усіх дій.

Стосовно допиту підозрюваного слід зазначи, що, як слушно вказує О. Мусієнко, під час його проведення варто встановити такі обставини: «…1) за яких обставин вчинено обман; 2) які способи застосовувалися (конкретні прийоми, операції, дії з підготовки, заволодіння майном тощо); 3) які ще злочини ним було вчинено; 4) хто і з якого часу брав участь у злочинній діяльності, яка роль кожного учасника обманних дій; 5) протягом якого періоду вчинявся злочин; 6) яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчиненого шахрайства; 7) який існував порядок розподілу грошових коштів у членів ОЗГ; 8) як оформлялися конкретні первинні бухгалтерські документи, який порядок відвантаження матеріальних цінностей; 9) чи є в них цінності, здобуті злочинним шляхом» [126, с. 158].

З огляду на наведене сформулюємо низку питань, котрі необхідно з’ясовувати під час допиту підозрюваного у межах розслідування кримінальних правопорушень, вчинених із використанням е-банкінгу, як-от:

– у який спосіб було вчинено протиправні дії;

– які способи використовувалися для входження у застосунок для е-банкінгу;

– протягом якого часу були скоєні кримінальні правопорушення та які

супутні протиправні діяння було вчинено;

– чи були вчинені протиправні дії у складі ОГ чи ЗО;

– якщо так, то які функції кожного з їхніх учасників та яка система розподілу грошових коштів між ними;

– які засоби застосовувалися під час учинення протиправних дій;

– яка загальна сума грошових коштів була на момент закінчення вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

На основі аналізу опитування респондентів [Додаток Б] нами було встановлено, що найбільш ефективними прийомами допиту підозрюваних в досліджуваній категорії кримінальних проваджень вони вважають такі:

– встановлення психологічного контакту з підозрюваним (100 %);

– переконання у потребі співпрацювати з уповноваженими особами та повідомлення правдивих показань (43 %);

– застосування різних темпів допиту (швидкого чи повільного) (34 %);

– неочікуване пред'явлення підозрюваному показань свідків (81 %);

– спостереження за поведінкою підозрюваного (49 %);

– застосування в ОГ чи ЗО конфліктів і протиріч (37 %);

– виявлення свідчень співучасників кримінального правопорушення (63 %);

– створення уявлення про інформованість уповноваженої особи (27 %);

– застосування відеозапису (51 %).

Досить цікавою вважаємо думку М. Павлика, який зауважував: «…враховуючи отриману інформацію, слідчий повинен тактично правильно визначити послідовність допитів, особливо, якщо злочини вчинялися у складі групи. Для цього слід максимально бути поінформованим відносно вікових, морально-психологічних характеристик, ролі та характеру участі кожного з учасників, враховувати їх зацікавленість у кінцевому результаті по справі. Як показує практика, більш ефективним є отримання в першу чергу показань від особи, яка, на думку слідчого, мала другорядну роль у вчиненні злочину та вчинила злочин вперше. Більш схильні до надання показань також особи, у

відношенні яких є велика кількість доказів. З метою тактичного впливу на учасника допиту, необхідно підготувати докази, які почергово пред'являтимуться під час допиту. Найбільш часто з цією метою використовуються висновки експертиз та різноманітні документи, в яких відображається доказова інформація, або документи, що були засобом вчинення злочину, а також інші предмети, що можуть бути речовими доказами» [134].

З-поміж найбільш ефективних тактичних прийомів допиту підозрюваного нами виділено залучення показань свідків та встановлення психологічного контакту. Вищенаведені тактичні прийоми мають застосовуватися, крім іншого, для вирішення конфліктних ситуацій. Щодо цього наведемо позицію В. Бедя, який відмічав, що «…конфліктна ситуація у процесі досудового слідства у кримінальній справі про будь-який злочин можлива завжди; це стосується і такої слідчої дії, як допит. Допит є ключовою слідчою дією, яка передбачає певною мірою протиборство і якій належить визначальна роль у встановленні істини, оскільки саме у процесі допиту має бути одержана надзвичайно важлива для слідства інформація про відомі допитуваному обставини справи та інші дані, що мають значення для встановлення істини. Протидія при проведенні допиту передбачає ту чи іншу форму спілкування суб'єкта протидії зі слідчим. У структурі спілкування розрізняють три компоненти: перцептивний, комунікативний та інтерактивний. Зміст перцептивного компонента складають процеси сприйняття і розуміння один одного учасниками спілкування. Комунікативний компонент складається з обміну інформацією учасників спілкування. Інтерактивний компонент характеризує взаємодію учасників спілкування» [6, с. 176].

Щодо категорій свідків, показання яких можна залучати до допиту підозрюваного, Я. Олійник виокремлював такі їх групи: «…громадяни, службові особи, які зробили повідомлення і заяви, що стали приводом і містили підстави для внесення відомостей в ЄРДР; особи, яким може бути

відома інформація про обставини і умови тих подій, які вони спостерігали, або умови і обставини тих дій, в яких вони брали участь; особи, які здійснювали підготовку документів щодо діяльності певного закладу; нотаріусів, які посвідчували установчі документи діяльності певного закладу; працівників органів державної реєстрації, територіальних органів державної податкової служби, державної статистики та державних цільових фондів, що реєстрували або ставили на облік цей заклад; працівників банківських установ, які відкривали та обслуговували рахунок організації» [131].

З приводу встановлення психологічного контакту з підозрюваними ми поділяємо думку К. Чаплинського, який відмічав, що нерідко на це «…негативно впливає поява захисників. Вони є висококваліфікованими їх союзниками, що необхідно враховувати під час проведення допитів. Участь захисника вносить певні складнощі і особливості у проведення усіх слідчих дій, а особливо – у тактику допиту. Захисник добре знає умови, механізм і можливості розслідування. Саме з урахуванням цих особливостей він здійснює захист інтересів підозрюваних (обвинувачених)» [194, с. 253].

З-поміж тактичних помилок, яких припускаються уповноважені особи під час реалізації СРД, НСРД та інших процесуальних заходів, необхідних для ефективного здійснення тактичних операцій у кримінальному провадженні, нами було виявлено такі:

– відсутність відповідних спеціалістів під час проведення окремих СРД, НСРД та інших процесуальних заходів;

– відсутність єдиного керівництва тактичною операцією;

– брак техніко-криміналістичних засобів та іншого необхідного обладнання для вилучення максимальної кількості доказової інформації.

Констатуючи вищенаведене, зазначимо, що тактичні операції стосовно збирання первинних даних про обставини злочинної події та виявлення ознак досліджуваних протиправних діянь повинні здійснюватися досить швидко та ефективно для забезпечення отримання максимально повної доказової інформації в досліджуваній категорії кримінальних проваджень.

3.2. Тактичні операції, спрямовані на встановлення та викриття осіб, які належать до події кримінального правопорушення, їх розшук та затримання

Встановлення особи злочинця має значення в кримінальних провадженнях будь-якої категорії. Для реалізації вказаного завдання проводиться низка процесуальних дій та заходів. Під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, встановлення особи злочинця не втрачає свого значення, навіть навпаки – важливість його лише збільшується, оскільки протиправні діяння вчинюються дистанційно – за допомогою мережі Інтернет. Крім того, особа може використовувати різноманітні способи приховування своєї протиправної діяльності, як-от: застосовування зміни ідентифікатора місця знаходження обладнання, за допомогою якого скоєні протиправні дії при застосовуванні е-банкінгу; маскування шпигунського програмного або технічного забезпечення під його законні аналоги тощо. Тому встановлення особи злочинця, його співучасників, а також їх розшук та затримання відіграє важливу роль у досліджуваній категорії кримінальних проваджень [114, с. 122].

У більшості випадків, як зазначалося вище, досліджувані протиправні діяння вчинюються дистанційно, тобто особу злочинця необхідно встановити. З приводу її встановлення окрема група науковців (Б. Лук'янчиков, Є. Лук'янчиков, С. Петряєв) зауважує, що у таких ситуаціях варто одержати наступні додаткові 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 неспівпадання 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)» [110, с. 475–476].

Водночас необхідно розуміти, що правопорушники для вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, обов'язково використовують електронно-обчислювальну техніку (комп'ютери, ноутбуки, смартфони). Тому при її знаходженні, як зазначає Д. Птушкін, потрібно, у тому числі, вилучати відео- або фотофайли, відомості про ведення переговорів у мережі Інтернет і електронною поштою, відвідування соціальних мереж, адреси потенційних жертв, графічні зразки бланків, значну кількість інформації про контакти, зв'язки тощо [152, с. 135].

У свою чергу, О. Мусієнко відмічає, що основна мета тактичної операції «Встановлення особи шахрая» – виявити особу чи групу осіб, що вчинили шахрайство. Це твердження повністю стосується і досліджуваної категорії протиправних діянь. Для реалізації вказаної тактичної операції авторка пропонує проводити такі слідчі (розшукові) дії, оперативно-розшукові та організаційні заходи, як: «…1) одержання всієї можливої інформації від підприємств, організацій, установ про особу, що підозрюється у вчиненні шахрайства; 2) допит свідків (осіб, пояснення яких є в первинних матеріалах); 3) слідчий огляд виробничих, торговельних, складських, службових приміщень; 4) обшук (при наявності підстав); 5) обшук за місцем проживання підозрюваних; 6) перевірка особи за оперативно-довідковими обліками МВС України; 7) виявлення можливих свідків; 8) зняття інформації з каналів зв'язку» [127, с. 142].

А вже О. Самойленко щодо здійснення тактичної операції «Персоналізація відомостей про особу/осіб злочинця/ів» наводить такий перелік дій і заходів: «…1) зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту; 2) встановлення місцезнаходження радіоелектронного засобу; 3) оформлення та відправлення запитів про витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових осіб відомостей, що становлять інтерес для кримінального провадження та/або здійснення запитів щодо обміну інформацією між компетентними підрозділами правоохоронних органів іноземних держав з питань реагування на кіберзлочини каналами сектору Національного контактного пункту реагування на кіберзлочини (НПК ДКП НП України)» [162, с. 53].

При цьому окрема група дослідників (Д. Максимус, О. Юхно) констатує, що «…номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор по визначенню входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання. Саме тому, завдяки наявності IP-адреси особи, яка представляє оперативний інтерес, можливо встановити місцезнаходження точки її доступу до Інтернету (країну, місто) та назву провайдера, який надає особі можливість такого доступу до Інтернету. Головним завданням, в даному випадку, виступає спосіб отримання IP-адреси особи, яка представляє оперативний інтерес. Основними способами є такі, як: запити до адміністрації звичайних (комерційних чи некомерційних) Інтернет-сайтів та використання легендованих Інтернет-сайтів» [111, с. 63].

Із приводу встановлення осіб, які вчинили комп'ютерне кримінальне

правопорушення, окрема група вчених-криміналістів (Б. Лук'янчиков, Є. Лук'янчиков, С. Петряєв) акцентує увагу на тому, що вказане є головним завданням розслідування. Крім того, автори зазначають, що дії уповноваженої особи зі встановлення факту доступу, способу і часу проникнення в комп'ютерну систему мають на меті й розшук особи, яка його вчинила. В розрізі визначеного дослідники наводять відповідний перелік слідчих (розшукових) дій, що їх потрібно проводити: огляд, обшук, допит, слідчий експеримент та ін., – для сприяння встановленню кола підозрюваних осіб [110, с. 477].

Ми підтримуємо думку І. Борисенка, який зауважує, що проведення дій зі встановлення місця перебування правопорушника та вжиття заходів стосовно його виявлення і затримання має бути об'єднане в єдиний тактичний комплекс. Автор відмічає, що «у плані розслідування слід намітити заходи щодо його розшуку, об'єднані з тактичною операцією «Пошук злочинця». У разі обізнаності слідчого про місця вірогідного перебування злочинця доцільно запланувати проведення тактичної операції «Затримання злочинця». Корисно скласти декілька варіантів плану затримання з урахуванням можливих змін обстановки і дій злочинця, що дозволяє звести до мінімуму ризик зриву операції» [17, с. 224].

Загалом затримання підозрюваного, як слушно зазначає В. Шепітько, повинно бути старанно підготовленим і несподіваним. Науковець констатує, що його необхідно проводити так, аби шахрай не зміг непомітно викинути чи знищити ті чи інші предмети, речі, документи. Одразу після затримання шахрая проводиться його обшук, а після – обшуки за місцем його проживання та роботи. Дослідник наголошує на тому, що у процесі обшуку реалізуються пошуки майна, одержаного шляхом обману, різного роду документів (у тому числі підроблених), інших предметів [85, с. 368–369].

Вважаємо слушним твердження Г. Захарової стосовно тактичної операції «Організація затримання злочинця, що діє в мережі Інтернет», яка зазначала, що «…у випадку, коли підозрювані у шахрайстві особи,

намагаючись уникнути кримінального покарання, переховуються від органів досудового розслідування, то всі слідчі (розшукові) та негласні слідчі (розшукові) дії повинні бути направлені на встановлення місця їх перебування. Для цього із застосуванням існуючих криміналістичних обліків та електронних реєстрів особливу увагу слід приділити також з'ясуванню істинних анкетних даних підозрюваних у шахрайстві осіб, з'ясуванню місця їх реєстрації та місця фактичного проживання, встановленню кола їх знайомих та родичів, встановленню спостереження за місцем можливої появи шахраїв, направленню запитів щодо встановлення фактів вчинення аналогічних шахрайських дій тощо» [47, с. 210].

У свою чергу, О. Пчеліна стосовно тактичної операції «Затримання злочинця» вказує, що така операція потребує ретельної організації із попередньою підготовкою, а також тісної взаємодії із працівниками оперативних підрозділів. Крім того, авторка відмічає, що вказана тактична операція може проводитися в комплексі з тактичною операцією «Розшук злочинця» або самостійно. На думку дослідниці, «…у першому випадку вона спрямована на вирішення завдання зі встановлення місцезнаходження злочинця, котрий переховувався від органів досудового розслідування та правосуддя. У другому випадку йдеться про фізичне захоплення (затримання) особи для забезпечення дієвості кримінального провадження» [153, с. 293].

Для оптимального та успішного затримання правопорушника обов'язковою умовою вважаємо застосування фактора раптовості. На думку Є. Пряхіна, у криміналістичній тактиці раптовість окреслюється як вибір найсприятливішого моменту для застосування тактичного прийому, що характеризується елементом несподіваності для певних учасників розслідування. Крім того, дослідник відмітив, що в іншому визначенні про раптовість вказується, що це засіб, який забезпечує непередбачуваність складу та характеру дій слідчого під час розслідування для сторони, яка протидіє, що надає йому тактичну ініціативу. Також вчений-криміналіст

зауважив, що окремі науковці розглядають раптовість під час проведення слідчих (розшукових) дій як несподіване повідомлення вибраної інформації, що створює умови для різкої зміни емоційного стану людини, котрий неможливо приховати від уповноваженої особи. Підсумовуючи, Є. Пряхін навів власне формулювання фактора раптовості як засобу, що може бути використаний однією зі сторін чи учасниками кримінального провадження в певний момент у формі активної дії (поведінки) та призводить до бажаного для ініціатора результату [84, с. 521]. Ми також вважаємо фактор раптовості обов'язковою складовою затримання особи, підозрюваної у вчиненні кримінального правопорушення, пов'язаного з використанням е-банкінгу.

Зі свого боку, О. Білоусов та С. Смоков зауважують, що визначена процесуальна дія «потребує ретельної підготовки та передбачає вжиття низки організаційно-підготовчих заходів, спрямованих на збирання даних щодо особи, яка підлягатиме затриманню, та визначення підрозділів, котрі будуть здійснювати затримання та координацію їх діяльності. При підготовці до затримання слідчий або оперативний працівник обов'язково моделює, тобто відтворює, умови, за яких буде протікати цей захід» [13, с. 19]. Як бачимо, потрібно з'ясувати низку аспектів для успішного проведення затримання правопорушника. З-поміж них варто виокремити такі: зібрати дані про особу, яка буде затримуватися; визначити характер її ймовірної поведінки; встановити коло її спілкування; вибрати час, місце та обстановку, в якій планується проводити затримання.

Щодо безпосереднього встановлення співучасників вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, досить доречною вбачаємо позицію О. Самойленко, яка визначила особливості тактичної операції «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи». На момент реалізації аналізованої операції, як зазначає авторка, персоналізація даних «…про особу/осіб злочинця/ів є закономірною, адже злочинця встановлено шляхом первинної перевірки інформації про злочин. До

структури операції «Встановлення та подолання засобів конспірації, які використовують учасники злочинної групи» належать такі дії: 1) контроль за вчиненням злочину; 2) здійснення за дорученням слідчого оперативним підрозділом оперативного (ініціативного) пошуку з метою встановлення характеру дій особи, що становить інтерес для кримінального провадження; 3) зняття інформації з транспортних телекомунікаційних мереж (електронних інформаційних систем) конкретного абонента» [163, с. 409].

А вже С. Кузьменко акцентує увагу на тому, що «…отримати певний обсяг відомостей про можливих злочинців, що сприятиме їх розшуку та успішному затриманню, можна в ході допитів свідків та потерпілих. Предметом допиту в основному є: анкетні дані злочинця (прізвище, ім'я, по батькові, місце проживання, місце роботи, сімейний стан, наявність судимостей, зокрема, за злочини у сфері економіки тощо); коло спілкування та особливості поведінки у суспільстві; місця, які особа найчастіше відвідує (коли саме, у якій компанії); наявність охорони, зброї, транспортного засобу тощо. Якщо допитуваний особисто не знайомий із підозрюваним, докладно слід описати зовнішні ознаки злочинця (фізичні властивості, манера поведінки, динамічні особливості, особливі прикмети, використання жаргонних висловів, наявність акценту тощо). Необхідно з'ясувати, за яких обставин відбулося знайомство і яка саме інформація відома про подію злочину» [94, с. 121–122].

Підсумовуючи, зазначимо, що встановлення особи злочинця має надзвичайно важливе значення під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, оскільки протиправні діяння вчинюються дистанційно – за допомогою мережі Інтернет. Також слід наголосити, що тактичні операції спрямовані на встановлення й затримання злочинців, збирання доказів, що доводять їхню причетність до протиправних дій та свідчать про характер злочинної діяльності, а також на з'ясування причетності до цього інших осіб. Пропонується проведення тактичної операції «Встановлення особи злочинця

та його співучасників, а також їх розшук і затримання» під час розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. На основі вищезазначених позицій науковців визначено заходи, котрі потрібно здійснювати для її реалізації, як-от:

– допити потерпілих;

– встановлення та допити свідків;

– огляд електронно-обчислювальної техніки;

– зняття інформації з електронних інформаційних систем або її частини;

– встановлення місцезнаходження радіоелектронного засобу;

– встановлення особи злочинця та подання його в розшук;

– встановлення місцезнаходження злочинця;

– затримання злочинця з дотриманням таких умов: зібрати дані про особу, яка буде затримуватися; визначити характер її ймовірної поведінки; встановити коло її спілкування; вибрати час, місце та обстановку, в якій планується проводити затримання;

– оформлення та відправлення вимог стосовно надання правоохоронними органами, органами державної влади та органами місцевого самоврядування інформації, що викликають інтерес для кримінального провадження за фактами вчинення протиправних діянь, пов’язаних із використанням е-банкінгу;

– обшуки за місцем проживання та в інших місцях перебування особи злочинця;

– допит підозрюваного для встановлення ймовірних співучасників кримінального правопорушення;

– проведення затримання співучасників;

– обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерполу, Європолу) стосовно реагування на кіберзлочини;

– призначення та проведення судових експертиз.

Для початку приділимо увагу тактиці допиту потерпілих і свідків, який є першочерговою СРД у комплексі заходів для оптимальної реалізації визначеної тактичної операції. Зокрема, було з'ясовано основні завдання допиту, як-от:

а) одержання відомостей для виявлення акаунта злочинця;

б) встановлення особливостей зв'язку потерпілого з правопорушником (особисте спілкування, соціальні мережі, телефонна розмова чи листування);

в) з'ясування контактної інформації про злочинця (номер телефону, е-гаманця, карткового рахунку, інстаграм-сторінки чи його електронної адреси тощо).

Крім того, під час допиту потерпілого доцільно пред'являти таку доказову інформацію:

а) скріншоти листування зі злочинцем;

б) скріншоти сторінок або облікового запису шахрая у месенджері;

в) скріншоти документів, що підтверджують сплату грошових коштів.

Необхідно пам'ятати, що проведення допитів знайомих та родичів правопорушника характеризується використанням тактичних прийомів, направлених на створення уявлення про необізнаність уповноваженої особи щодо факту вчиненого протиправного діяння. Зокрема, слід застосовувати метод побічного допиту, під час якого встановлюються питання, які, з одного боку, не стосуються вчиненого кримінального правопорушення з використанням е-банкінгу, а з іншого – направлені на отримання доказових даних.

Крім того, в попередньому підрозділі нами було визначено особливості тактики огляду. А зараз вважаємо доречним окреслити вузлові ділянки, на яких розташовані сліди протиправних дій, як-от:

1) місце розташування ЕОТ, яка була застосована під час учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу;

2) розташування терміналів, відділення банку, банкоматів тощо;

3) локації програмно-технічних засобів, на які було спрямовано

протиправні дії.

Також слід наголосити на тактиці огляду віртуальної інформації, що знаходиться у відкритому доступі у мережі Інтернет чи перебуває на матеріальних носіях даних або відповідних сервісах зберігання вказаних даних. Зокрема, при огляді ЕОТ (комп'ютера, смартфона, планшета) об'єктом є як сама техніка, так і носії даних (кеш-пам'ять, програми, системні дані, cookies браузерів тощо).

З приводу проведення НСРД вважаємо слушним твердження В. Лисенка та О. Лисенка, які вказували, що проведення НСРД «…для встановлення місця перебування розшукуваних осіб має специфічну мету, яка відмінна від випадків їх проведення для отримання доказової інформації у кримінальному провадженні. У ході проведення таких дій діяльність правоохоронних органів, перш за все, спрямована на отримання інформації, що може бути використана для встановлення конкретного місця знаходження особи, що розшукується, та його безпосереднього затримання. Варто зауважити, що за результатами проведення негласних слідчих (розшукових) дій у розшуковій роботі слідчого нерідко встановлюється доказова інформація щодо вчинених злочинів, а також факти вчинення інших суспільно-небезпечних діянь, про які не було раніше відомо правоохоронним органам. Кожна із негласних слідчих (розшукових) дій у розшуковій роботі слідчого має специфічне спрямування і за результатами їх проведення може бути отримана різноманітна інформація. В ході проведення аудіо-, відеоконтролю особи (ст. 260 КПК України) можливо отримати таку інформацію: дані щодо фактичного місця проживання розшукуваної особи; номер його мобільного телефону; особливості зв'язку родичів, знайомих із розшукуваною особою тощо. Окрім зазначеного проведення такої дії сприяє отримати інформацію щодо речових доказів та інших доказів, які стосуються вчиненого злочину» [105, с. 119]. У свою чергу, Р. Благута та М. Остапчук зазначили, що «…одним із способів реалізації тактичної операції «Затримання злочинця» як наслідку документування та реалізації

оперативної розробки є проведення такого виду НСРД, як контроль за учиненням злочину» [14, с. 63]. Отже, акцентуємо увагу на обов'язковій реалізації таких НСРД, як зняття інформації з електронних інформаційних систем або її частини та встановлення місцезнаходження радіоелектронного засобу. Проведення зазначених заходів зумовить оптимальне отримання орієнтуючої інформації для подальшого здійснення необхідних процесуальних дій.

А вже О. Татаров вказував, що «…на етапі реформування органів кримінальної юстиції в Україні забезпечити належний прокурорський нагляд та судовий контроль за негласними актами розслідування з метою дотримання гарантованих Конституцією прав і свобод та унеможливлення здійснення безпідставного проведення НСРД не вдасться повною мірою, що зумовлює зловживання та використання НСРД як засобу досягнення особистих інтересів окремих правоохоронців. Тож у нашій державі потрібен комплексній підхід» [185, с. 28].

Слушною вважаємо позицію О. Лисенка, який зазначав: про факт того, що злочинець переховується від слідства та суду, «…може свідчити те, що особа не з'являється за викликами до органів досудового розслідування; за місцем реєстрації чи фактичного проживання не перебуває; не з'являється за місцем роботи (навчання, лікування тощо); відсутність інформації про надходження такої особи до травматологічних пунктів, моргів; відсутність особи на стаціонарному лікуванні в лікувальних закладах; відсутність особи за місцем проживання сім'ї, батьків, друзів тощо. В рамках тактичної операції «Розшук злочинця» також підлягають перевірці дані про осіб: щодо яких застосовано адміністративний арешт; затриманих на підставі положень ст. 207–213 КПК України; щодо яких застосовані запобіжні заходи на підставі ст. 176–206 КПК України; призваних для проходження служби в армії чи для проходження військових зборів тощо» [106, с. 192].

Зі свого боку, О. Здоровко зауважував, що «…у випадках, коли злочинець не затриманий, необхідно використовувати тактичну операцію

«Пошук злочинця», метою якої є виявлення вбивці. Така тактична операція може включати до свого складу: а) організацію переслідування по «гарячих» слідах; б) виявлення очевидців та їх опитування; в) використання словесного портрета й складання композиційного портрета; г) виявлення місць можливого перебування злочинця; ґ) призначення судових експертиз; д) використання криміналістичних обліків; е) організацію оперативно-розшукових заходів, спрямованих на встановлення винних у певному кримінальному середовищі; є) вивчення матеріалів справ про злочини минулих років; ж) обшук-затримання; з) проведення групового обшуку» [52, с. 32].

У свою чергу, М. Думчиков зауважував, що «…цифровізація всіх сфер діяльності в криміналістиці може бути розглянута в декількох аспектах: – використання цифрових технологій для підвищення ефективності пошуково-пізнавальної діяльності слідчого, ефективної організації цієї діяльності на сучасному рівні, оптимізації взаємодії різних органів, установ при розслідуванні злочинів; – використання інформаційно-комунікативних технологій для розслідування злочинів. Широке поширення інформаційних комп’ютерних технологій сприяє подальшим розробкам в області алгоритмізації процесу розслідування злочину в цілому і окремих його етапів; – рішення дидактичних завдань в сфері підготовки, перепідготовки, підвищення кваліфікації слідчих, слідчих-криміналістів, судових експертів, обміну досвідом» [31, с. 104–105].

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

допиту спеціалісти можуть заперечувати проти поставлених запитань учасниками кримінального провадження, що беруть участь у допиті при розслідуванні банківських злочинів» [214, с. 457].

Також нами визначено, що тимчасовий доступ до речей і документів для подальшого вилучення майна та огляд речей (ЕОТ, планшетів, смартфонів) дозволить вирішувати такі завдання:

1) з'ясування списку задіяної ЕОТ у кримінальних правопорушеннях, пов'язаних із використанням е-банкінгу;

2) визначення необхідного програмного забезпечення для неї;

3) розгляд платіжних процесів для знаходження латентних замаскованих платежів;

4) вирішення питання доступу до акаунтів (особистих, банківських), що були створені для здійснення е-банкінгу.

Спеціальні знання використовуються більшою чи меншою мірою під час розслідування усіх категорій кримінальних правопорушень. Водночас особливості конкретних протиправних діянь зумовлюють специфічність їх застосування. Так, розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, характеризується обов'язковим залученням спеціалістів у галузі комп'ютерних та інформаційних технологій, а також проведенням різних видів судової комп'ютерно-технічної експертизи [117, с. 139].

Загалом, найбільш правильним вважаємо формулювання Б. Романюка, який визначив спеціальні знання як «…сукупність науково обґрунтованих відомостей окремого (спеціального виду), якими володіють особи – спеціалісти у рамках будь-якої професії у різних галузях науки, техніки, мистецтва та ремесла і відповідно до норм кримінально-процесуального законодавства використовують їх для успішного вирішення завдань кримінального судочинства» [159, с. 57].

Зі свого боку, окрема група авторів сформулювала дефініцію «спеціальні знання», що використовуються під час розслідування шахрайств,

котрі вчиняються з використанням ЕОТ, як комплекс знань і навичок, із-поміж яких як окремі правові, так і у вузькій (спеціальній) галузі науки, техніки (зокрема, комп'ютерних технологій, криміналістики тощо), отриманих у процесі фахової підготовки та професійної діяльності, якими володіють особи-спеціалісти і відповідно до норм кримінального процесуального законодавства використовують із витратою часу й інтелектуальних зусиль у взаємозв'язку з науково-технічними засобами для успішного виконання завдань кримінального провадження, встановлення вагомих обставин, що мають доказове значення [29, с. 51]. Як бачимо, друге формулювання дещо розширює визначення досліджуваного терміна шляхом звуження виду спеціальних знань до комп'ютерних технологій.

Досить цікавим у розрізі зазначеного вважаємо твердження групи дослідників, які вказали, що «…у цьому разі залучений спеціаліст-бухгалтер або економіст звертає увагу слідчого на фрагменти документів, де відображено важливу інформацію для слідства, а також спеціаліст допомагає правильно зафіксувати ці дані у протоколі. Крім того, спеціалісти допомагають слідчому обрати лише потрібні документи для розслідування із значної їх кількості. Слідчий разом зі спеціалістами при огляді документів має можливість оперативно отримати потрібну інформацію про показники виконання плану, стан обліку та звітності. Крім того, після огляду спеціалісти допомагають слідчому сформулювати питання для проведення економічної експертизи» [184, с. 160–161].

А вже І. Коваленко відмічав, що «…XXI сторіччя можна впевнено назвати «комп'ютерним сторіччям». Стрімкий розвиток інформаційних технологій полегшив життя людства та, в свою чергу, породив нові кримінальні правопорушення в сфері інформаційних технологій. Всесвітня мережа Інтернет стала для всього людства невід'ємною частиною життя. За допомогою Інтернету люди спілкуються по всьому світу за допомогою соціальних мереж, месенджерів. Ще 20 років тому це було практично нереально, сьогодні – це звичайні речі. Ці зміни також стосуються і

банківського сектору. Зокрема, для того, щоб провести платіж, у більшості випадків використовується Internet banking. Тобто, для того, щоб сплатити будь-які послуги, не потрібно йти у відділення банку – це все можна зробити за декілька секунд, маючи доступ до Інтернету» [63, с. 262].

Інший дослідник, В. Давиденко виокремлює дві форми використання спеціальних знань. На думку автора, перша з них визначена кримінальним процесуальним законодавством (судові експертизи, участь фахівців у підготовці та проведенні СРД), а друга – не передбачена законом (консультативно-довідкова діяльність фахівців в окремих галузях знань) [25, с. 180]. У свою чергу, В. Тіщенко також вирізняє дві форми використання спеціальних знань, як-от: безпосередня, тобто така, що безпосередньо спрямована на збирання й отримання доказів; опосередкована, тобто та, що сприяє збиранню й оцінці доказів [183, с. 351–352].

Цікавою є й думка Т. Коршикової, яка на основі вивчення досліджень вчених-криміналістів дійшла висновку, що «…до основних форм використання спеціальних знань під час досудового розслідування шахрайств з використанням ЕОТ відносяться: залучення спеціаліста до проведення процесуальних дій та залучення експерта для надання висновків з питань, що виникають під час кримінального провадження – процесуальна форма. Серед непроцесуальних (організаційних) форм найбільш дієвими є консультативно-довідкова та аналітична допомога фахівця у відповідній сфері (насамперед фахівця з питань комп’ютерних технологій)» [77, с. 180].

Зі свого боку, Д. Пашнєва вказує, що «…форми використання спеціальних знань можуть бути диференційовані на обов’язкове і факультативне залучення їх при проведенні процесуальних дій». Крім того, як зазначає автор, процесуальні форми використання спеціальних знань поділяються за характером дій, при проведенні яких вони застосовуються, на ті, що використовуються при проведенні слідчих та інших процесуальних дій. Непроцесуальні форми застосування спеціальних знань можуть бути поділені за ознаками сфери використання і суб’єкта їх застосування [140, с. 89].

Найбільш слушною в розрізі нашого дослідження ми вбачаємо позицію С. Чучка, який із-поміж основних форм використання спеціальних знань виокремив такі, як: «…а) безпосереднє використання уповноваженою особою спеціальних знань під час проведення окремих слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій; б) призначення судових експертиз; в) залучення спеціаліста до проведення окремих процесуальних дій. Залучення відповідних спеціалістів для проведення окремих слідчих (розшукових) дій забезпечує максимальну ефективність їх проведення. Зокрема, огляд веб-сторінки, на якій розміщено повідомлення про товари, які особа пропонує купити, з проведенням подальшого експертного дослідження у сфері телекомунікації, по-перше, надає змогу вивчити зміст інформації стосовно діяльності шахраїв та характеру пропонованої продукції; по-друге, зафіксувати IP-адресу комп'ютерного обладнання, з якого здійснювалось управління веб-сайтом; по-третє, визначити Інтернет-провайдера, який надавав доступ до веб-сайту» [203, с. 239].

Особливо важливою, на думку групи дослідників (Н. Павлова, Д. Птушкін, К. Чаплинський), є участь спеціаліста при проведенні слідчих (розшукових) дій, у ході яких ведеться пошук і вилучається інформація, що міститься в комп'ютерах, мобільних телефонах, інших електронних пристроях. Автори вказують, що часто комп'ютерна техніка, мобільні телефони захищені паролем, який ускладнює доступ до інформації від сторонніх осіб. У цьому випадку до огляду зазначеної техніки необхідно залучати фахівця, як правило, програміста, який зможе надати допомогу щодо увімкнення зазначеної техніки [138, с. 133].

Доречним вбачаємо твердження групи науковців, які вказали, що факти та обставини, котрі виявляються у процесі аналізу апаратно-технічних засобів та програмного забезпечення, встановленого на цих засобах, які є доказами у матеріалах кримінального провадження, є предметом СКТЕ [33, с. 118–119]. Також стосовно можливого призначення

та проведення судових експертиз звернемося до Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень, де вказано: «…до основних завдань експертизи комп'ютерної техніки і програмних продуктів належать: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку» [146].

У свою чергу, Є. Наливайко засвідчила, що «…на даний час, проаналізувавши експертну практику, можливо пересвідчитися у постійному збільшенні кількості експертних завдань щодо пошуку на комп'ютерних носіях інформації, яка стосується роботи користувача персонального комп'ютера (ПК) у глобальній мережі Інтернет, тобто звернення його на конкретні сайти, хронології чи історії звернень тощо. Це зумовлено збільшенням кількості кримінальних проваджень, пов'язаних з противоправним поширенням у глобальній мережі певної інформації, у тому числі кримінального характеру (щодо торгівлі людьми, розповсюдження порнографічних зображень тощо). Вважаємо за необхідне наголосити на невідповідність тяжкості покарання передбаченому у законодавстві України у вказаній категорії злочинів, що також не є стримуючим фактором у діях злочинців, тобто міра покарання практично усіх злочинах не перевищує середню тяжкість, а отже, не завжди можливо застосування НСРД. Як приклад, у Іспанії лише за перетинання границі з фальшивими кредитними карточками, борговими картками чи акредитивами передбачене покарання від восьми до десяти років позбавлення волі та штраф у десятикратному розмірі підроблених грошей» [128, с. 100].

Як вказують окремі дослідники (Н. Карпінська, О. Крикунов), однією з головних проблем наразі під час проведення СКТЕ є питання

підтвердження компетентності осіб, які проводять згаданий вид експертиз, які володіють спеціальними знаннями в галузі інформації та які не є співробітниками державних судово-експертних установ [57, с. 144].

Зазначимо, що у вищенаведених науково-методичних рекомендаціях визначено такий перелік питань, що можуть вирішуватися під час проведення вказаних експертиз: «…Чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить) і у якому вигляді? Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача? Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації? Чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія? Яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)? Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)? Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст)? Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме – встановлене, не встановлене) програмне забезпечення? Які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому? Чи можливо виконання певних дій за допомогою даного програмного продукту? Чи можливе вирішення певного завдання за допомогою даного програмного продукту? Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?» [146].

Також слід наголосити, що «…для дослідження інформації, що міститься 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» [146].

Підсумовуючи, зазначимо, що нами було окреслено особливості призначення і проведення судових експертиз при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу (судової комп'ютерно-технічної експертизи, програмно-комп'ютерної та інформаційно-комп'ютерної експертиз).

Висновки до розділу 3

Після опрацювання питань організації та проведення тактичних операцій під час розслідування досліджуваних кримінальних правопорушень варто сформулювати такі висновки:

1. На основі аналізу праць низки науковців (А. Жилін, С. Кузьменко, О. Мусієнко, Н. Павлова, А. Рейнгольд) запропоновано підхід до розгляду методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, крізь призму проведення комплексів тактичних операцій. Тактична операція являє собою комплекс процесуальних дій та заходів, які спрямовані на розв'язання певного тактичного завдання, що відіграє важливу роль під час розслідування кримінальних правопорушень.

2. Виокремлено завдання, що їх потрібно вирішувати для здійснення тактичних операцій стосовно збирання первинної інформації про обставини події та виявлення ознак кримінального правопорушення, як-от: обставини, що передували вчиненню протиправних дій; способи вчинення протиправних дій (фішинг, застосування шпигунських програм, спам-ботів); електронно-обчислювальна техніка, яка використовувалася для здійснення протиправних дій; час і тривалість злочинних дій; учасники, їхня кількість і роль кожного в учиненні протиправних дій; загальна кількість потерпілих та їх характеристика.

3. Надано перелік тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов’язаних із використанням е-банкінгу. Запропоновано низку питань, які необхідно з’ясовувати під час допиту підозрюваного, як-от: у який спосіб було вчинено протиправні дії; які способи використовувалися для входження у застосунок для е-банкінгу; протягом якого часу були скоєні кримінальні правопорушення та які супутні протиправні діяння було вчинено; чи були вчинені протиправні дії у складі ОГ чи ЗО; якщо так, то які функції кожного з їх учасників та яка система розподілу грошових коштів між ними; які засоби застосовувалися під час учинення протиправних дій; якою була загальна сума грошових коштів на момент закінчення вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, та ін.

4. Вказано на найбільш ефективні тактичні прийоми допиту підозрюваного. Наголошено на їх обов’язковому використанні під час вирішення конфліктних ситуацій допиту.

5. Охарактеризовано особливості реалізації комплексу слідчих (розшукових) дій, НСРД, процесуальних і розшукових заходів та інших дій, направлених на реалізацію визначеної тактичної операції. Наголошено, що тактичні операції спрямовані на встановлення й затримання злочинців, збирання доказів, що доводять їхню причетність до протиправних дій та свідчать про характер злочинної діяльності, а також на з’ясування

причетності до цього інших осіб. Значну увагу приділено тактиці допиту потерпілих і свідків, який є першочерговою СРД у комплексі заходів для оптимальної реалізації визначеної тактичної операції.

6. З'ясовано основні завдання допиту, зокрема: а) одержання відомостей для виявлення акаунта злочинця; б) встановлення особливостей зв'язку потерпілого з правопорушником (особисте спілкування, соціальні мережі, телефонна розмова чи листування); в) з'ясування контактної інформації про злочинця (номер телефону, е-гаманця, карткового рахунку, інстаграм-сторінки чи його електронної адреси тощо). Під час допиту потерпілого доцільно пред'являти таку доказову інформацію: а) скріншоти листування зі злочинцем; б) скріншоти сторінок або облікового запису шахрая у месенджері; в) скріншоти документів, що підтверджують сплату грошових коштів.

7. Визначено особливості тактики огляду. Виділено вузлові ділянки, на яких розташовані сліди протиправних дій, як-от: 1) місце розташування ЕОТ, що була застосована під час учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу; 2) розташування терміналів, відділення банку, банкоматів тощо; 3) локації програмно-технічних засобів, на які було спрямовано протиправні дії. Наголошено на тактиці огляду віртуальної інформації, що знаходиться у відкритому доступі у мережі Інтернет чи перебуває на матеріальних носіях даних або відповідних сервісах зберігання вказаних даних. Зокрема, при огляді ЕОТ (комп'ютера, смартфона, планшета) об'єктом є як сама техніка, так і носії даних (кеш-пам'ять, програми, системні дані, cookies браузерів тощо).

8. Акцентовано увагу на обов'язковій реалізації НСРД – зняття інформації з електронних інформаційних систем або її частини та встановлення місцезнаходження радіоелектронного засобу. Проведення зазначених заходів зумовить оптимальне отримання орієнтуючої інформації для подальшого здійснення необхідних процесуальних дій.

9. Визначено, що тимчасовий доступ до речей і документів для

подальшого вилучення майна та огляд речей (ЕОТ, планшетів, смартфонів) дозволить вирішувати такі завдання: 1) з'ясування списку задіяної ЕОТ у кримінальних правопорушеннях, пов'язаних із використанням е-банкінгу; 2) визначення необхідного програмного забезпечення для неї; 3) розгляд платіжних процесів для знаходження латентних замаскованих платежів; 4) вирішення питання доступу до акаунтів (особистих, банківських), що були створені для здійснення е-банкінгу. Окреслено особливості призначення і проведення судових експертиз при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу (як-от: судова комп'ютерно-технічна експертиза, програмно-комп'ютерна та інформаційно-комп'ютерна експертизи).

Основні результати розділу опубліковано у працях [114; 117; 121].

ВИСНОВКИ

У дисертації надано теоретичне узагальнення і сучасне опрацювання наукового завдання, що виявляється у розробленні теоретико-прикладних основ методики розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу, та визначення науково обґрунтованих практичних рекомендацій та пропозицій стосовно розвитку цих основ та покращення з огляду на практику зарубіжних країн. У результаті дослідження вироблено низку теоретичних положень, висновків та практичних рекомендацій, першорядними з яких виокремити такі:

1. Здійснено криміналістичний аналіз проведення електронних операцій у сфері використання банківських електронних платежів. Охарактеризовано фактори, що впливають на вчинення протиправних дій. Динаміка звернень до правоохоронних органів за фактами вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, дедалі зростає та набуває все більш прихованого та організованого характеру. Дієві заходи із запобігання злочинним проявам не відповідають сучасним загрозам.

Визначено сучасні наукові підходи до розуміння сутності та системи криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням е-банкінгу.

Запропоновано систему окремої методики розслідування, до якої включено складові з огляду на організаційно-тактичні особливості реалізації кримінальних проваджень, розпочатих за фактом учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, як-от: криміналістична характеристика; розгляд первинної інформації, а також особливості занесення відповідних даних до Єдиного реєстру досудових розслідувань; обставини, котрі варто з’ясовувати під час розслідування; типові слідчі ситуації та інші.

Окреслено структуру криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням е-банкінгу, елементами якої є:

спосіб та обстановка учинення кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого.

Доведено, що наведені складові мають сталі кореляційні зв'язки та важливе значення для початкового етапу розслідування з огляду на можливість висунення слідчих версій та проведення невідкладних слідчих (розшукових) дій та НСРД.

2. Охарактеризовано обстановку та систематизовано типові способи й сліди вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

З'ясовано, що способи злочинної діяльності мають широкі межі та виявляються у системі взаємопов'язаних дій із підготовки, безпосереднього вчинення й приховування протиправних дій, що пов'язані між собою єдиними мотивом і метою. Систематизовано підготовчі дії, а також зосереджено увагу на способах приховування досліджуваної категорії протиправних діянь.

Виявлено й охарактеризовано типові способи вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, зокрема: 1) протиправні дії при застосовуванні е-банкінгу; 2) протиправні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 3) протиправні дії з відомостями, що знаходяться у пам'яті електронно-обчислювальної техніки; 4) поширення шпигунських програмних чи технічних засобів, а також їх збут із застосовуванням мережі Інтернет.

Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, характеризується умовами часу та місця, що здебільшого не мають чітких територіальних і часових меж. Визначено найбільш розповсюджені місця вчинення злочинних дій. До обстановки віднесено такі складові: 1) час, протягом якого здійснювалися злочинні дії; 2) час, коли настали наслідки від протиправних дій; 3) місце реалізації злочинних дій (віртуальне середовище, в якому вчиняються дії, і місця, де

знаходяться точки доступу, – IP-адреси).

Слідова картина кримінальних правопорушень, пов’язаних із використанням е-банкінгу, охоплює 3 групи слідів: 1) матеріальні сліди, що містяться на різноманітних матеріальних носіях інформації (квитанції, банківські картки, сім-картки, паперові копії даних з ЕОТ, відбитки папілярних ліній на ЕОТ, клавіатурі банкомата); 2) ідеальні сліди, що становлять відомості у пам’яті потерпілих, підозрюваних та осіб, які були свідками незаконних операцій із використанням е-банкінгу; 3) віртуальні сліди (пам’ять ЕОТ, кеш-пам’ять серверів інтернет-провайдерів, пам’ять смартфонів, кеш-пам’ять електронного реєстру термінала чи банкомата тощо).

3. З’ясовано криміналістично вагомі ознаки особи злочинця, визначено та охарактеризовано віктимогенні групи потерпілих.

Сформовано ймовірний «портрет» особи злочинця. З’ясовано, що особам, які вчиняють кримінальні правопорушення, пов’язані з використанням е-банкінгу, притаманні високий рівень інтелекту, винахідливість та комунікабельність. Властивою характеристикою особи злочинця (хакери, фішери, фрікери, спамери, кіберсквотери, спеціалісти з програмного забезпечення та використання ЕОТ) є особливий вид ознак – інтелектуальні. Ці особи мають спеціальні знання й навички у сфері електронного бізнесу, е-комерції, інтернет-торгівлі, здійснення банківських операцій, використання цифрових технологій, комп’ютерного програмування та ін. Здебільшого це чоловіки віком 20–40 років, які мають базову або повну вищу освіту.

Виокремлено віктимогенні групи потерпілих.

4. Конкретизовано особливості початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. Встановлено, що початкові відомості, котрі стали приводом для внесення інформації до ЄРДР за фактом учинення кримінальних правопорушень, які надійшли до правоохоронних органів, визначають напрямки розслідування.

Вирізнено типові слідчі ситуації, що формуються на початковому етапі розслідування кримінальних правопорушень: 1) вчинено кримінальне правопорушення, пов'язане з використанням е-банкінгу, наявна достатня кількість доказової інформації, встановлено особу злочинця – 7 %; 2) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, особу злочинця не встановлено – 62 %; 3) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, встановлено особу злочинця, але злочинні дії замасковані під легальну фінансову діяльність – 8 %; 4) вчинено кримінальне правопорушення, наявна заява потерпілої особи, відсутня будь-яка доказова інформація – 23 %.

5. Визначено особливості взаємодії слідчих та працівників оперативних підрозділів Національної поліції України у кримінальному провадженні.

Встановлено найбільш розповсюджені форми взаємодії, зокрема: здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів (91 %); обмін інформацією (83 %); надання уповноваженій особі відомостей, що зібрані у процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення відомостей до ЄРДР (65 %); групове планування розшукових заходів (31 %); здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, що мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними матеріалами (29 %).

У кримінальному провадженні вагомого значення набуває використання обміну інформацією як однієї з найбільш ефективних форм взаємодії, особливо в умовах запровадженого воєнного стану.

Така інформація може стосуватися наступних обставин: а) ознак злочинного діяння, пов'язаного з використанням е-банкінгу; б) структури ОГ та ЗО, що здійснюють тривалу злочинну діяльність в економічній сфері; в) характерних ознак злочинців, які здійснюють протиправну діяльність.

6. Виокремлено заходи профілактичної діяльності працівників правоохоронних органів (слідства, дізнання, кіберполіції) щодо виявлення й усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а саме: 1) повідомлення громадян за допомогою засобів масової інформації про юридичну відповідальність за вчинені протиправні дії; 2) встановлення осіб, схильних до антисуспільної поведінки у сфері використання ЕОТ, а також їх подальше занесення до обліку в підрозділах кіберполіції; 3) участь працівників кіберполіції у тематичних передачах, круглих столах, ток-шоу, де висвітлюються питання запобігання протиправним діям у кіберпросторі; 4) вивчення матеріалів кримінальних проваджень для з'ясування та усунення умов і причин, що сприяли вчиненню протиправних діянь; 5) інформування громадян у соціальних мережах, ЗМІ, месенджерах щодо фактів учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (як-от: фішинг, кардинг, спамінг).

Вирізнено причини та умови, що впливають на вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Встановлено, що однією з головних причин неефективності заходів із запобігання кримінальним правопорушенням, пов'язаним із використанням е-банкінгу, залишається низький рівень обізнаності слідчих та працівників оперативних підрозділів Національної поліції України щодо типових злочинних схем під час здійснення незаконних банківських операцій та напрямів збирання електронних доказів, встановлення правопорушників за цифровою слідовою картиною, особливостей документування злочинних дій у кіберпросторі тощо.

7. Розкрито тактичні операції щодо збирання первинних даних про обставини злочинної події та виявлення ознак досліджуваних протиправних діянь, а саме з-поміж них визначено такі, як: «Встановлення характеру події кримінального правопорушення», «З'ясування місця та часу вчинення протиправного діяння», «Встановлення способу вчинення протиправного

діяння (фішинг, застосування шпигунських програм, спам-ботів)», «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», «З'ясування особи потерпілого та її віктимної поведінки, а також перевірка їх зв'язків» та ін.

Виокремлено завдання, котрі потрібно вирішувати для ефективного проведення відповідних тактичних операцій.

На основі узагальнення судово-слідчої практики запропоновано перелік слідчих (розшукових) дій, НСРД та інших процесуальних заходів, необхідних для ефективного здійснення тактичних операцій у кримінальному провадженні. Виявлено тактичні помилки, яких припускаються уповноважені особи під час реалізації таких операцій.

8. Сформовано перелік заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», як-от: 1) допити потерпілих; 2) встановлення очевидців злочинної події та допити свідків; 3) огляд електронно-обчислювальної техніки; 4) зняття інформації з електронних інформаційних систем або її частини; 5) встановлення місцезнаходження радіоелектронного засобу; 6) встановлення особи злочинця та оголошення її у розшук; 7) встановлення місцезнаходження злочинця; 8) затримання злочинця; 9) направлення вимог щодо надання правоохоронними органами, органами державної влади та органами місцевого самоврядування інформації, котра має значення для кримінального провадження за фактами вчинення протиправних діянь, пов'язаних із використанням е-банкінгу; 10) обшуки за місцем проживання та в інших місцях перебування злочинця; 11) допит підозрюваного для встановлення ймовірних співучасників кримінального правопорушення (лідера та активних учасників ОЗГ); 12) проведення затримання співучасників, залучених до злочинної діяльності; 13) обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерполу, Європолу) стосовно реагування на кіберзлочини; 14) призначення та проведення судових експертиз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк О. А. Методика розслідування кримінальних правопорушень проти громадського порядку: наукові та праксеологічні засади : монографія. Херсон : Видавничий дім «Гельветика», 2020. 352 с.

2. Антонюк О. А. Наукові диспути стосовно профілактики під час розслідування кримінальних правопорушень проти громадського порядку. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. Т. 2. С. 177–182.

3. Астахова О. О. Значення обстановки вчинення злочину як ознаки об’єктивної сторони злочину. *Юридична наука*. 2015. № 7. С. 91–98.

4. Баланюк О. В. Підготовка до злочину: поняття та криміналістична класифікація. *Актуальні проблеми держави і права*. 2006. Вип. 27. С. 192–196.

5. Бахін В., Лук’янчиков Б. Склад і призначення криміналістичної характеристики злочинів. *Часопис Донецькоко університету*. 2000. Вип. 1 (4). С. 37–45.

6. Бедь В. В. Юридична психологія : навч. посібник. Львів : Новий Світ, 2000. 376 с.

7. Безруков Д. В. Використання оперативно-технічних засобів щодо протидії злочинам проти власності підрозділам карного розшуку : дис. ... канд. юрид. наук : 12.00.09 / Донецький юридичний інститут МВС України. Кривий Ріг, 2015. 230 с.

8. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*. 2019. Т. 70. № 2. С. 313–331.

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

10. Біленчук П. Д., Біленчук Д. П., Міщенко В. Б., Мотлях О. І.

Національна безпека України: сучасні інформаційні технології і можливі джерела безпеки. *Вісник Академії праці і соціальних відносин ФП України*. 1998. № 1. С. 61–72.

11. Біленчук П. Д., Перкін В. І. Тактичні прийоми, тактичні комбінації та тактичні операції в розслідуванні злочинів : навч. посібник. Київ : УАВС, 1996. 32 с.

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

13. Білоусов О. І., Смоков С. М. Затримання підозрюваного у кримінальному процесі України : монографія. Одеса, 2009. 112 с.

14. Благута Р. І., Остапчук М. С. Формування та застосування типових тактичних операцій під час розслідування розбоїв. *Молодий вчений*. 2016. № 8 (35). С. 59–65.

15. Бойко А. О., Чещевий Є. І., Безрук В. В. Алгоритмізація процесу підвищення безпеки проведення фінансових операцій в мережі Інернет. *Вісник Сумського державного університету. Серія : Економіка.* 2017. № 3. С. 152–158.

16. Бойко О. П. Взаємодія слідчих з підрозділами карного розшуку на досудовому провадженні : автореф. дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 20 с.

17. Борисенко І. Організація та проведення тактичних операцій при розслідуванні вбивств. *Вісник Академії правових наук України*. 2001. № 3 (26). С. 213–225.

18. Борідько О. А., Гаркуша А. М. Сутність сучасної концепції профілактики злочинів органами внутрішніх справ. *Актуальні проблеми розбудови кримінально-процесуального судочинства України : зб. наук. статей.* Херсон : Мрія, 2003. С. 173–175.

19. Боровик А. В., Копотун І. М. Кіберзлочини в Україні

(кримінально-правова характеристика) : навч. посібник. Луцьк : СПД Гадяк Ж. В., друкарня «Волиньполіграф», 2019. 304 с.

20. Брич Л. Місце вчинення злочину і його значення у розмежуванні складів злочинів та відмежуванні їх від складів інших правопорушень. *Вісник Львівського університету. Серія юридична.* 2011. Вип. 52. С. 267–280.

21. Буждиганчук Є. Ю. Деякі аспекти криміналістичного аналізу обстановки вчинення сутенерства організованою групою. *Сутність та значення впливу законодавства на розвиток суспільних відносин : матеріали Міжнародної науково-практичної конференції* (м. Одеса, 13–14 березня 2020 р.). Одеса : ГО «Причорноморська фундація права», 2020. С. 122–125.

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

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

24. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. 18 с.

25. Давиденко В. С. Спеціальні знання в розслідуванні економічних злочинів. *Юридичний часопис Національної академії внутрішніх справ.* 2016. № 2 (12). С. 178–188.

26. Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис… канд. юрид. наук : 12.00.09 / Університет «Одеська юридична академія». Одеса, 2014. 20 с.

27. Діброва Т. А., Пісенко Д.О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний*

журнал. № 11. 2022. С. 546–549. URL : http://lsej.org.ua/11_2022/132.pdf.

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

29. Доказування у справах про злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки : метод. рекомендації. Київ : Нац. акад. внутр. справ, 2020. 60 с.

30. Дубно Т. В. Співвідношення способу вчинення злочину та злочинної дії. *Форум права*. 2011. № 4. С. 224–228.

31. Думчиков М. О. Процеси діджиталізації і криміналістика : ретроспективний аналіз. *Криміналістика і судова експертиза.* 2020. Вип. 65. С. 100–108.

32. Душейко Г. О. Організаційно-тактичні основи реалізації оперативно-розшукової інформації в стадії порушення кримінальної справи : автореф. дис. … канд. юрид. наук : 12.00.09. Харків, 2001. 19 с.

33. Експертизи у судочинстві України : наук.-практ. посібник / за заг. ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2014. 504 с.

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

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

38. 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 : Дніпроп. держ. ун-т внутр. справ, 2021. С. 275–276.

39. Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020. № 2. Т. 2. С. 209–215.

40. Жилін А. Е. Взаємодія різних підрозділів правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів: актуальні питання. *KELM*. 2023. № 3. С. 119–123.

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

42. Жилін А. Е. Наукові диспути стосовно тактичних операцій щодо збирання початкових відомостей про обставини події та виявлення ознак шахрайства у сфері використання банківських електронних платежів. *Вісник Львівського торговельно-економічного університету*. *Юридичні науки*. 2023. № 13. С. 134–138.

43. Журавель В. А. Криміналістичні методики : сучасні наукові концепції. Харків : Вид. агенція «Апостіль», 2012. 304 с.

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

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

46. 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. 20 с.

47. Захарова Г. В. Організація і тактика проведення окремих слідчих (розшукових) дій при розслідуванні шахрайства у сфері туризму, вчиненого організованою групою. *Науковий вісник публічного та приватного права*. 2019. Вип. 2. Т. 3. С. 209–214.

48. Заяць К. Д. Методика розслідування шахрайств : дис. … канд. юрид. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2020. 196 с.

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

50. Здоровко С. Ф. Тактичні операції при розслідуванні вбивств, що вчиняються організованими групами і злочинними організаціями : автореф. дис. … канд. юрид. наук : 12.00.09 / Національна юридична академія імені Ярослава Мудрого. Харків, 2002. 18 с.

51. Здоровко С. Ф. Тактичні операції при розслідуванні вбивств, що вчиняються організованими групами і злочинними організаціями : дис… канд. юрид. наук : 12.00.09 / Національна юридична академія імені Ярослава Мудрого. Харків, 2002. 209 с.

52. Здоровко С. Ф. Типові тактичні операції при розслідуванні вбивств, вчинених організованими злочинними групами : метод. рекомендації. Харків : Національна юридична академія ім. Я. Мудрого, 2002. 40 с.

53. Зелінський А. Ф. Кримінологія : навч. посібник. Київ : Рубікон, 2000. 240 с.

54. Іванов В. В. Взаємодія оперативних підрозділів органів внутрішніх справ і слідчого на досудових стадіях кримінального процесу : автореф. дис.

… канд. юрид. наук : 21.07.04. Київ, 1998. 20 с.

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

56. Капцош В. Я. Стан та особливості розвитку Інтернет-торгівлі товарами в міжнародному вимірі. *Науковий вісник Ужгородського національного університету*. 2017. № 13 (1). С. 115–119.

57. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1 (9). С. 140–144.

58. Карпов Н. С. Криміналістична характеристика торгівлі людьми. *Університетські наукові записки*. 2005. № 3 (15). С. 268–273.

59. Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України : звіт про НДР (проміжний) / кер. О. В. Кузьменко. Суми : СумДУ, 2018. 199 с. URL : https://essuir.sumdu.edu.ua/bitstream-download/123456789/73900/1/Kuzmenko_1414.pdf.

60. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан ; за ред. О. Денькович, Г. Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL : law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf.

61. Кіберполіція. Кібербезпека України. *WikiLegalAid*. URL : https://wiki.legalaid.gov.ua/index.php/Кіберполіція._Кібербезпека_України (дата звернення – 12.12.2023).

62. Кобилянська Л. М. Кіберзлочинність як глобальна загроза економічній безпеці сучасної держави. *Науковий вісник Херсонського державного університету.* 2014. Вип. 8. Ч. 5. С. 14–17.

63. 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.

64. 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 науково-практичного семінару* (м. Дніпро, 28 травня 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. С. 145–147.

65. Коваленко І. О. Організаційно-практичне забезпечення проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Visegrad Journal on Human Rights.* 2019. № 6. С. 117–122.

66. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 Право / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2022. 234 с.

67. Коваленко І. О. Сутність та система криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів. *Науковий вісник Дніпропетровського державного університету внутрішніх справ* . 2022. № 3. С. 363–368.

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

69. Козаченко І. П., Регульский В. Л. Правові, морально-етичні та організаційні основи оперативно-розшукової діяльності. Львів : Львів. ін-т внутр. справ при Нац. акад. внутр. справ України, 1999. С. 178–203.

70. Козицька О. Особа потерпілого як елемент криміналістичної характеристики злочинів, вчинених відносно дітей. *Підприємництво, господарство і право*. 2016. № 11. С. 202–206.

71. Комаров М. Огляд кібератак на об’єкти критичної інфраструктури. *Національна академія наук України. Інститут проблем моделювання в*

енергетиці. Електронне моделювання. 2019. Т. 41. № 6. С. 91–106.

72. Комаров М. Ю. Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури : дис. … канд. техн. наук : 05.13.05 / Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. Київ, 2021. 171 с.

73. Комаров М. Ю., Гончар С. Ф., Ониськова А. В. Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури. *Моделювання та інформаційні технології.* 2018. № 82. С. 40–48.

74. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського Національного Університету. Серія : Право.* 2021. Вип. 68. С. 220–224.

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

76. 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.

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

78. Костенко М. В. Щодо особливостей розслідування злочинів, вчинених організованими групами. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО»*. 2017. Вип. 24. С. 148–150.

79. Кравченко О. В. Психологічні особливості шахрайства : автореф. дис. ... канд. психол. наук : 19.00.06 / Національний університет внутрішніх справ. Харків, 2005. 21 с.

80. Краус К. М., Краус Н. М., Манжура О. В. Електронна комерція та Інтернет-торгівля : навч.-метод. посібник. Київ : Аграр Медіа Груп, 2021. 454 с.

81. Кривопуск О. Г. Способи вчинення злісного невиконання обов'язків по догляду за дитиною або за особою, щодо якої встановлена опіка чи піклування. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 3. С. 369–376.

82. Криміналістика : підруч. для слухачів, ад'юнктів, викладачів вузів системи МВС України / Біленчук П. Д., Дубовий О. П., Салтевський М. В., Тимошенко П. Ю. ; за ред. П. Д. Біленчука. Київ : АТІКА, 1998. 416 с.

83. Криміналістика : підруч. / за заг. ред. В. В. Пясковського. 2-е вид., перероб. і доп. Харків : Право, 2020. 752 с.

84. Криміналістика : підруч. / за заг. ред. Є. В. Пряхіна. 3-є вид., перероб. та доп. Львів : ЛьвДУВС, 2016. 948 с.

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

86. Криміналістика : підруч. : 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.

87. Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

88. Кримінальний кодекс України : наук.-практ. коментар / за заг. ред. В. В. Сташиса, В. Я. Тація. Київ : Концерн «Видавничий Дім «Ін Юре», 2003. 1196 с.

89. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text.

90. Кримінологія : підруч. для студ. вищ. навч. закл. / Джужа О. М., Кондратьєв Я. Ю., Кулик О. Г., Михайленко П. П. та ін. ; за заг. ред. О. М. Джужи. Київ : Юрінком Інтер, 2002. 352 с.

91. Кримінологія: Загальна та Особлива частини : підруч. 2-е вид.,

перероб. і доп. / за заг. ред. В. В. Голіни. Харків : Право, 2009. 288 с.

92. Кримінологія і профілактика злочинів : курс лекцій у 2 кн. Особлива частина / Александров Ю. В. та ін. Київ : Національна академія внутрішніх справ України, 2000. 201 с.

93. Кузьменко С. С. Розслідування шахрайства, пов'язаного з інвестуванням коштів у будівництво об'єктів нерухомості : автореф. дис. … канд. юрид. наук : 12.00.09 / Відкритий міжнародний університет розвитку людини «Україна». Київ, 2019. 20 с.

94. Кузьменко С. С. Розслідування шахрайства, пов'язаного з інвестуванням коштів у будівництво об'єктів нерухомості : дис. … канд. юрид. наук : 12.00.09 / Відкритий міжнародний університет розвитку людини «Україна». Київ, 2019. 249 с.

95. Кузьмічов В. С., Прокопенко Г. І. Криміналістика : навч. посібник / за заг. ред. В. Г. Гончаренка та Є. М. Моїсеєва. Київ : Юрінком Інтер, 2001. 368 с.

96. Кулик С. Г. Кримінологічна характеристика та запобігання злочинам проти моральності : дис. … канд. юрид. наук : 12.00.08 / Класичний приватний університет. Запоріжжя, 2016. 266 с.

97. Куратченко М. В. Обстановка вчинення сутенерства та втягнення особи в заняття проституцією. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2016. № 3. С. 236–242.

98. Куратченко М. В. Розслідування сутенерства та втягнення особи в заняття проституцією : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2017. 192 с.

99. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : автореф. дис. … канд. юрид. наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2002. 16 с.

100. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : дис. … канд. юрид. наук : 12.00.09 / Національна юридична

академія України імені Ярослава Мудрого. Харків, 2002. 227 с.

101. Курман О. В. Особливості криміналістичної характеристики шахрайства з фінансовими ресурсами. *Вісник Запорізького юридичного інституту*. 2002. № 1. С. 195–201.

102. Курс кримінології: Загальна частина : підруч. : у 2 кн. / за заг. ред. О. М. Джужи. Кн. 1. Київ : Юрінком Інтер, 2001. 352 с.

103. Латиш К. В. Тактичні операції діагностичного рівня під час розслідування вандалізму. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2016. Вип. 40. Т. 2. С. 114–117.

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

105. Лисенко В. В., Лисенко О. В. Негласні слідчі (розшукові) дії у розшуковій роботі слідчого. *Сучасні тенденції розвитку криміналістики та кримінального процесу*. Харків, 2017. С. 118–120.

106. Лисенко О. В. Організація розшуку осіб, які переховуються від органів досудового слідства та суду. *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2013. № 4 (63). С. 189–195.

107. Логінова В. В. Поняття та значення особи злочинця в методиці розслідування тілесних ушкоджень. *Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах : матеріали Міжнародної науково-практичної конференції* (м. Запоріжжя, 5 листопада 2010 р.) : у 2 ч. Ч. 1. Запоріжжя : ЗЮІ ДДУВС, 2010. С. 115–118.

108. Локтіонова В. В. Ознаки об’єктивної сторони злочину та місце серед них злочинних наслідків. *Право і суспільство*. 2012. № 1. С. 249–254.

109. 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.

110. Лук’янчиков Б. Є., Лук’янчиков Є. Д., Петряєв С. Ю.

Криміналістика : навч.посібник для студ. юрид. спец. вищ. навч. закл. : в 2 ч. Ч. II : Криміналістична тактика. Методика розслідування. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2017. 505 с.

111. Максимус Д. О., Юхно О. О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посібник. Харків : НікаНова, 2013. 102 с.

112. Малютін Е. В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Т. 2. С. 143–147.

113. Малютін Е. В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія : Право.* 2022. № 2. С. 232–236.

114. Малютін Е. В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Т. 2. С. 122–128.

115. Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146.

116. Малютін Е. В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

117. Малютін Е. В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 139–141.

118. Малютін Е. В. Особливості початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням е-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. 171–173.

119. Малютін Е. В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 425–428. URL : http://www.lsej.org.ua/9_2021/9_2021.pdf.

120. Малютін Е. В. Спосіб учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 77–82.

121. Малютін Е. В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

122. Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ : навч. посібник / за заг. ред. Є. В. Пряхіна. Львів : ЛьвДУВС, 2011. 324 с.

123. Микитчик А. В. Заходи запобігання кіберзлочинності в Україні.

Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. Міжнародної науково-практичної конференції до 25-річчя ХНУВС (м. Харків, 18 квітня 2019 р.) / МВС України ; Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 137–139.

124. Міжнародна поліцейська енциклопедія : у 8 т. / відп. ред. : В. В. Черней, В. Я. Тацій, Ю. С. Шемшученко, Ю. І. Римарпенко. Т. 8 : Інформаційно-аналітична, освітня та наукова діяльність, психологічні засади поліцейської служби, міжнародне співробітництво. Київ : Атіка, 2010. 1132 с.

125. Мотлях О. І. Питання організації планування дій слідчого у злочинах, вчинених у сфері комп'ютерних технологій. *Вісник Академії адвокатури України*. 2005. Вип. 2. С. 113–120.

126. Мусієнко О. Л. Допит свідків при розслідуванні шахрайства. *Проблеми законності.* 2007. Вип. 91. С. 156–161.

127. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. В. Ю. Шепітька. Харків : Право, 2010. 168 с.

128. Наливайко Є. О. Криміналістичні та процесуальні особливості у злочинах пов'язаних із кіберзлочинністю. *Актуальні питання протидії кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукраїнської науково-практичної конференції* (м. Харків, 17 листопада 2017 р.) / МВС України ; Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2017. С. 98–101.

129. Настільна книга слідчого : наук.-практ. видання для слідчих і дізнавачів / Шепітько В. Ю. та ін. 2-е вид., перероб. і доп. Київ : Вид. Дім «Ін Юре», 2007. 728 с.

130. Никифорчук Д. Й. Проблемні питання взаємодії в розкритті злочинів. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2002. № 5. С. 151–154.

131. Олійник Я. О. Допит свідків, підозрюваних та обвинувачених під

час розслідування умисного знищення або пошкодження об'єктів житлово-комунального господарства. *Держава і право. Юридичні і політичні науки.* 2012. Вип. 56. С. 432–437.

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

133. Охрімчук Т. В. Способи вчинення шахрайства з фінансовими ресурсами. *Правова держава : історія, сучасність та перспективи формування в Україні : матеріали III Всеукраїнської науково-практичної конференції* (м. Запоріжжя, 23 квітня 2010 р.). Запоріжжя : Юридичний ін-т ДДУВС, 2010. Ч. II. С. 94–96.

134. Павлик М. П. Розслідування злочинів у сфері надання послуг із працевлаштування за кордоном : дис. … д-ра філос. : 081 Право / Національна академія внутрішніх справ. Київ, 2021. 241 с.

135. Павлова Н. В. Особливості розслідування шахрайства, пов'язаного з відчуженням приватного житла : дис. ... канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпропетровськ, 2007. 223 с.

136. Павлова Н. В. Розслідування шахрайства при укладанні цивільно-правових угод щодо відчуження житла : монографія. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ, 2008. 176 с.

137. Павлова Н. В. Співвідношення понять «тактична операція» та «тактична комбінація» у криміналістиці. *Актуальні питання криміналістики : матеріали Всеукраїнської науково-практичної конференції* (м. Київ, 20 грудня 2019 р.). Київ : Нац. акад. внутр. справ, 2019. С. 166–169.

138. 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.

139. Павлова Н. В., Рец В. В. Визначення місця та часу вчинення

шахрайства на первинному ринку нерухомості. *Науковий вісник Дніпропетровського університету внутрішніх справ.* 2018. № 3 (66). С. 139–143.

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

141. Погорецький М. А., Хотенець В. М. Процесуальні і організаційно-тактичні форми взаємодії органів дізнання і досудового слідства. *Право і безпека*. 2002. № 1. С. 178–183.

142. Попов К. Л. Соціально-психологічні орієнтири у віктимологічному дослідженні жертви шахрайства. *Наукові праці Національного авіаційного університету. Серія : Юридичний вісник «Повітряне і космічне право».* 2015. № 1 (34). С. 164–169.

143. Попова І. М. Розслідування шахрайств, пов'язаних із залученням коштів громадян на будівництво житла : автореф. дис. ... канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2011. 20 с.

144. Попова І. М. Розслідування шахрайств, пов'язаних із залученням коштів громадян на будівництво житла : дис. ... канд. юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2011. 250 с.

145. Приловський В. В. До питання здійснення профілактичних заходів працівниками правоохоронних органів стосовно виявлення та усунення причин і умов втягнення неповнолітніх у протиправну діяльність. *Юридична наука*. 2019. № 11. С. 191–197.

146. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 р. № 53/5. URL : https://zakon.rada.gov.ua/laws/show/z0705-98#Text.

147. Про затвердження Положення про Єдиний реєстр досудових

розслідувань, порядок його формування та ведення : наказ Офісу Генерального прокурора № 298 від 30.06.2020. URL : https://zakon.rada.gov.ua/laws/show/v0298905-20#Text.

148. Профілактика злочинів : підруч. Київ : Атіка, 2010. 967 с.

149. Профілактика правопорушень (кримінологічні та експертно-криміналістичні аспекти) : монографія / Мельник П. В., Данкович Н. О., Фрідман І. Я. та ін. Ірпінь : Національний університет ДПС України, 2011. 170 с.

150. Птушкін Д. А. Віктимність поведінки потерпілих у справах про шахрайства, пов'язані із заволодінням нерухомим майном громадян. *Актуальні проблеми кримінального права, кримінології та кримінально-виконавчого права : матеріали Всеукраїнської науково-практичної конференції* (м. Дніпро, 25 травня 2018 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. С. 97–99.

151. Птушкін Д. А. Допит потерпілого при розслідуванні шахрайств відносно об'єктів нерухомого майна громадян: обставини, які підлягають встановленню. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2015. Вип. 34. Ч. 2. С. 99–102.

152. Птушкін Д. А. Розслідування шахрайства, вчиненого щодо об'єктів нерухомого майна громадян : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 240 с.

153. Пчеліна О. В. Тактичні операції під час розслідування злочинів у сфері службової діяльності. *Підприємництво, господарство і право*. 2017. № 3. С. 290–294.

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

155. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : автореф. дис. … канд. юрид. наук : 12.00.09 /

Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 20 с.

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

157. Рейнгольд А. В. Оцінка первинної інформації на початку розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 1. Т. 2. С. 18–23.

158. Римарчук Г. С., Мельник В. І. Юридична природа кіберзлочинів. *Науковий вісник Ужгородського національного університету*. 2014. Вип. 24. Т. 4. С. 54–57.

159. Романюк Б. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві : монографія. Київ : Національна академія внутрішніх справ України, 2002. 196 с.

160. Саінчин О. С. Криміналістичні умови розкриття умисних вбивств. *Правова держава*. 2008. № 10. С. 267–273.

161. Салтевський М. В. Криміналістика : підруч. : у 2 ч. Харків : Консум, 2001. Ч. 2. 528 с.

162. Самойленко О. А. Діяльність правоохоронних органів у протидії кіберзлочинності : навч.-метод. посібник. Одеса : Національний університет «Одеська юридична академія», 2020. 133 с.

163. Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* 2015. № 4. С. 408–411.

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

165. Самойлов С. В. Консультативна та довідкова діяльність обізнаних осіб як форма застосування та використання спеціальних знань при розслідуванні шахрайств, учинених з використанням мережі «Інтернет».

Держава і право в умовах судової реформи : матеріали Всеукраїнської науково-практичної конференції студ., аспірантів і молодих учених (м. Донецьк, 8 квітня 2011 р.). Донецьк : Донецький університет економіки і права, 2011. С. 257–259.

166. 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.

167. Самойлов С. В. Про деякі способи вчинення шахрайств з використанням мережі Інтернет. *Правові проблеми державотворення і захисту прав людини в Україні : матеріали Міжнародної науково-практичної конференції* (м. Харків, 23–24 лютого 2011 р.) : у 4 т. Харків : ГО «Асоціація аспірантів-юристів», 2011. Т. 3. С. 104–108.

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

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

170. Самсонова В. В., Пиріг І. В. Методика розслідування крадіжок, вчинених на території садівницьких товариств і дачних кооперативів : монографія. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. 212 с.

171. Севідов О. А. Криміналістична класифікація суб’єктів кіберзлочинів та їх особливості. *Актуальні питання розслідування кіберзлочинів : матеріали Міжнародної науково-практичної конференції* (м. Харків, 10 грудня 2013 р.) / МВС України ; Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2013. С. 164–169.

172. Селезньова О. М. Теоретико-методологічні основи інформаційного права України : монографія. Чернівці : Місто, 2014. 407 с.

173. Сенаторов М. В. Потерпілий від злочину в кримінальному праві :

автореф. дис. … канд. юрид. наук : 12.00.08 / Національна юридична академія імені Ярослава Мудрого. Харків, 2005. 20 с.

174. Сенаторов М. В. Потерпілий від злочину в кримінальному праві : монографія / за наук. ред. В. І. Борисова. Харків : Право, 2006. 208 с.

175. 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. Вип. 5. С. 151–156.

176. Сіренко О. В. Обстановка вчинення крадіжок, грабежів і розбійних нападів неповнолітніми як елемент криміналістичної характеристики. *Науковий вісник Національного університету державної податкової служби України (економіка, право).* 2012. № 4 (59). С. 223–228.

177. Справа № 456/1471/22. Архів Стрийського міськрайонного суду Львівської обл. 2022.

178. Справа № 524/5260/21. Архів м. Кременчука Полтавської обл. 2022.

179. Справа № 535/2260/22. Архів Котелевського районного суду Полтавської обл. 2023.

180. Справа № 570/699/22. Архів Рівненського районного суду Рівненської обл. 2022.

181. Справа № 727/21/23. Архів Шевченківського районного суду м. Чернівці. 2023.

182. Справа № 742/4475/23. Архів Прилуцького міськрайонного суду Чернігівської обл. 2024.

183. Степанюк Р. Л. Теоретичні засади методики розслідування злочинів, вчинених у бюджетній сфері України : дис. … д-ра юрид. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2012. 491 с.

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

185. Татаров О. Ю. Інститут негласних слідчих (розшукових) дій: проблеми протидії злочинності. *Науковий вісник Національної академії внутрішніх справ.* 2015. № 3. С. 25–32.

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

187. Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : дис. … д-ра юрид. наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2003. 476 с.

188. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

189. Тіщенко В. В. Щодо використання спеціальних знань у кримінальному провадженні. *Матеріали Всеукраїнської науково-практичної Інтернет-конференції* (м. Одеса, 27 листопада 2013 р.). Одеса : «Юридична література», 2013. С. 349–353.

190. Тюптя Л. Т., Іванова І. Б. Соціальна робота (теорія і практика). Київ : Університет «Україна», 2004. 407 с.

191. Узунова О. В., Логвиненко А. В. Проблеми реформування кримінального судочинства. URL : https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/23035/1/ПРОБЛЕМИ%20РЕФОРМУВАННЯ%20КРИМІНАЛЬНОГО%20СУДОЧИНСТВА.pdf.

192. Хижняк Є. С. Типові слідчі ситуації при розслідуванні статевих злочинів. *Південноукраїнський правничий часопис*. 2012. № 4. С. 197–199.

193. Царьов Р. Ю. Електронна комерція : навч. посібник з підготовки бакалаврів. Одеса : ОНАЗ ім. О. С. Попова, 2010. 112 с.

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

195. Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни:

психологічний практикум : практ. посібник / Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023. 80 с. URL : https://ispp.org.ua/wp-content/uploads/2023/09/posib_chaplinska_2023.pdf.

196. Чередник К. О. Розслідування шахрайства на ринку нерухомості, вчиненого злочинними угрупованнями : автореф. дис. … канд. юрид. наук : 12.00.09 / Відкритий міжнародний університет розвитку людини «Україна». Київ, 2019. 20 с.

197. Чередник К. О. Розслідування шахрайства на ринку нерухомості, вчиненого злочинними угрупованнями : дис. … канд. юрид. наук : 12.00.09 / Відкритий міжнародний університет розвитку людини «Україна». Київ, 2019. 270 с.

198. Чередник К. О. Тактичні операції, спрямовані на вилучення та дослідження документальних джерел інформації про ознаки шахрайства на ринку нерухомості, вчиненого злочинними угрупованнями. *Прикарпатський юридичний вісник*. 2018. № 1. Т. 3. С. 178–183.

199. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. ... д-ра юрид. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2010. 34 с.

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

201. 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.

202. Чорний А. М. Тактичні операції при розслідуванні умисних вбивств. *Право і суспільство*. 2011. № 2. С. 238–242.

203. Чучко С. В. Використання спеціальних знань при розслідуванні шахрайств при купівлі-продажу товарів через мережу Інтернет. *Право і*

суспільство. 2021. № 2. С. 234–240.

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

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

206. Чучко С. В. Способи вчинення шахрайства, пов’язаного із придбанням товарів через мережу Інтернет. *Visegrad Journal on Human Rights*. 2019. № 6. Vol. 3. С. 234–238.

207. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 1 (32). С. 213–225.

208. Шевчук В. М. Структура тактичних операцій : проблеми та пропозиції. *Вісник Академії правових наук України*. 2012. № 4. С. 318–328.

209. Шевчук В. М. Технологія тактичної операції як різновид криміналістичних технологій. *Вісник Національної академії правових наук України*. 2013. № 4 (75). С. 235–242.

210. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: юридичні науки.* 2018. Т. 29 (68). № 6. С. 119–124.

211. Шепітько В. Ю. Особа потерпілого в системі криміналістичної характеристики злочинів. *Проблеми законності.* 2008. Вип. 93. С. 168–174.

212. Шеремет А. П. Криміналістика : навч. посібник для студ. вищ. навч. закл. 2-е вид. Київ : Центр учбової літератури, 2009. 472 с.

213. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : монографія. Харків : Харків юридичний, 2010. 319 с.

214. Яремчук В. О. Криміналістичні та спеціальні знання при розслідуванні кримінальних правопорушень у банківській сфері. *Юридичний науковий електронний журнал*. 2022. № 6. С. 456–458. URL : http://lsej.org.ua/6_2022/6_2022.pdf.

215. Яровенко Г. М., Бояджян М. М. Аналіз наслідків кібершахрайств в банківській системі України. *Гроші, фінанси і кредит.* 2018. Вип. 18. С. 836–843.

216. Brenner S. W. Cybercrime Investigation and Prosecution : the Role of Penal and Procedural Law. University of Dayton School of Law. 2001. URL : https://www.researchgate.net/publication/240610895_Cybercrime_Investigation_and_Prosecution_the_Role_of_Penal_and_Procedural_Law.

217. Chaplynskyi K., Yefimov M., Pletenets V., Harashchuk D., Demchenko I. Features of interaction between law enforcement agencies during the investigation of criminal offenses according to international standards. *Cuestiones Politicas*. 2023. Vol. 41. Issue 76. P. 469–481.

218. Khamyha Yu. Financial pyramids as a type of financial fraud: theoretical-motivational aspect. *European Journal of Economics and Management*. 2020. Vol. 6. Issue 3. P. 15-22.

219. Shelley L. I. Organized Crime, Terrorism and Cybercrime. URL : https://www.ojp.gov/ncjrs/virtual-library/abstracts/organized-crime-terrorism-and-cybercrime.

220. 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*. 2021. Special Issue. № 2 (114). P. 114–119.

221. Yefimov M., Pavlova N., Fedchenko V., Pletenets V., Kryvopusk O. Foreign experience in legal regulation of fraud investigation. *Revista De La Universidad Del Zulia*. 2022. Vol. 13. Issue 38. P. 159–168.

ДОДАТКИ

Додаток А

Результати вивчення

215 кримінальних проваджень із проблематики дослідження у таких областях: Вінницька, Дніпропетровська, Донецька, Закарпатська, Запорізька, Івано-Франківська, Київська, Львівська, Миколаївська, Одеська, Полтавська, Сумська, Тернопільська, Харківська, Херсонська, Черкаська, Чернівецька – та в м. Київ

№	Досліджувані питання	%
	КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА	
1	**Обстановка вчинення кримінального правопорушення**	
	1.1. Місце вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу:	
	1) не мають конкретно визначеного місця події	**74**
	2) мають конкретне місце події	**26**
	З них:	
	1) місця розміщення ЕОТ, що була застосована для вчинення протиправних дій (смартфон, комп'ютер, ноутбук, планшет)	**74**
	2) місця розташування банкоматів, банків, а також інших підприємств фінансової сфери	**16**
	3) місце перебування потерпілої особи, на яку були спрямовані протиправні дії	**9**
	4) інші	**1**
2	**Способи вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу**	
	2.1. Повноструктурний	**100**

	2.2. Підготовка до вчинення	**100**
	1) знаходження потрібної електронно-обчислювальної техніки (ноутбуків, комп'ютерів, планшетів)	
	2) підготовка слушних обставин для реалізації протиправних дій та ін.	
	3) виготовлення шпигунських технічних або програмних засобів для протиправного використання під час здійснення операцій е-банкінгу	
	4) збут чи розповсюдження без необхідного дозволу мережею Інтернет відомостей, що мають значення під час здійснення операцій е-банкінгу	
	2.3. Способи безпосереднього вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу	**100**
	1) протиправні дії при застосовуванні е-банкінгу	
	2) протиправні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення	
	3) протиправні дії з відомостями, що знаходяться в пам'яті електронно-обчислювальної техніки	
	4) поширення шпигунських програмних чи технічних засобів, а також їх збут із застосовуванням мережі Інтернет	
	2.4. Способи приховування	**100**
	1) ліквідація устаткування, що застосовувалося для скоєння протиправних дій	**39**
	2) надання завідомо неправдивих показів під час здійснення процесуальних дій (так само як і неправдиве алібі)	**45**
	3) відмова від надання показів	**58**
	4) маскування шпигунського програмного або технічного забезпечення під його законні аналоги	**46**

	5) застосовування зміни ідентифікатора місця знаходження обладнання, за допомогою якого були скоєні протиправні дії при застосовуванні е-банкінгу	**78**
3	**Відомості про слідову картину протиправного діяння**	
	3.1 Матеріальні слід	**34**
	3.2. Електронні сліди (віртуальні, цифрові, комп'ютерні)	**100**
	3.3. Ідеальні сліди	**41**
5	**Особа потерпілого**	
	5.1. Віктимогенні групи потерпілих:	
	1) фізичні особи, які здійснювали купівлю-продаж товарів і послуг на онлайн-платформах та інтернет-аукціонах із використанням е-банкінгу	
	2) працівники фінансових установ, підприємств та організацій різних форм власності	
	3) їхні клієнти	
	4) родичі клієнтів	
	5) юридичні особи – при здійсненні матеріально-технічного постачання та інших заходів у випадках використання інтернет-банкінгу	
6	**Дані про особу злочинця**	
	6.1. Стать:	
	1) чоловіча	**81**
	2) жіноча	**19**
	6.2. Вік:	
	1) від 16 до 20 років	**9**
	2) від 20 до 30 років	**34**
	3) від 30 до 40	**31**
	4) від 40 до 50	**20**
	5) особи віком 50 років і старше	**6**

	6.3. Освіта:	
	1) базова середня	**3**
	2) повна середня	**5**
	3) професійно-технічна	**12**
	4) базова вища	**38**
	5) вища	**42**
	6.4. Сімейний стан:	
	1) у шлюбі	**37**
	2) ні	**63**
	6.5. Рід занять:	
	1) учень (студент)	**18**
	2) працюючий	**76**
	3) у сфері фінансової діяльності та сфері комп'ютерних технологій	**71**
	6.6. Наявність судимості	**6**
	6.7. Кримінальні правопорушення вчинено у стані сп'яніння:	
	1) алкогольного	**1**
	2) наркотичного	**1**
	6.8. Особи, які вчиняють кримінальні правопорушення, пов'язані з використанням е-банкінгу, відрізняються досить високим інтелектуальним рівнем:	
	1) так	**91**
	2) ні	**9**

	ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ	
7	**Початкові відомості, які стали приводом для внесення інформації до ЄРДР за фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, надійшли до відповідних підрозділів правоохоронних органів у такий спосіб:**	
	1) заяви, листи та повідомлення від громадян, які є потерпілими від зазначених кримінальних правопорушень	**79**
	2) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене кримінальне правопорушення або стали свідками його скоєння	**8**
	3) повідомлення працівників установ, підприємств та організацій	**3**
	4) матеріали досудового розслідування, виділені з інших кримінальних проваджень	**4**
	5) матеріали, отримані під час проведення НСРД або розшукових заходів	**7**
8	**Типові слідчі ситуації початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу:**	
	1) вчинено кримінальне правопорушення, пов'язане з використанням е-банкінгу, наявна достатня кількість доказової інформації, встановлено особу злочинця	**7**
	2) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, особу злочинця не встановлено	**62**
	3) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, встановлено особу злочинця, але злочинні дії замасковані під легальну фінансову діяльність	**8**
	4) вчинено кримінальне правопорушення, наявна заява потерпілої особи, відсутня будь-яка доказова інформація	**23**

	СЛІДЧІ (РОЗШУКОВІ) ДІЇ, НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ТА ІНШІ ПРОЦЕСУАЛЬНІ ДІЇ:	
9	**Які СРД та процесуальні дії проводились:**	
	1) огляд місця події	**86**
	2) допит потерпілого або представника потерпілої сторони	**100**
	3) огляд електронної інформації	**95**
	4) допит свідка	**100**
	5) тимчасовий доступ до речей і документів	**74**
	6) допит підозрюваного	**100**
	7) обшук	**89**
	8) призначення та проведення експертиз	**100**
	9) слідчий експеримент	**2**
	10) пред'явлення особи для впізнання	**6**
	а) за голосом	**3**
	б) у натурі	**1**
	в) за фото	**2**
	11) одночасний допит раніше допитаних осіб	**63**
	12) огляд документів	**57**
10	**Огляд:**	
	9.1. Проводився:	
	1) місце розташування ЕОТ, що була застосована під час учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу	
	2) розташування терміналів, відділення банку, банкоматів тощо	
	3) локації програмно-технічних засобів, на які було спрямовано протиправні дії	
11	**Обшук:**	
	10.1. Об'єкти, що вилучались:	
	1) ЕОТ	

	2) фотографії, відеозаписи, на яких наявні дані, що мають значення для кримінального провадження	
	3) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб	
12	**Які НСРД проводилися найчастіше:**	
	1) спостереження за об’єктом	
	2) прослуховування телефонних переговорів	
	3) зняття інформації з електронних інформаційних систем або її частини	
	4) встановлення місцезнаходження радіоелектронного засобу	
13	**Допит:**	
	13.1. Ситуації за конфліктністю:	
	1) безконфліктні	**21**
	1) конфліктні	**79**
14	**Одночасний допит:**	**82**
	14.1. Між ким проводився:	
	1) між підозрюваним та потерпілим	**89**
	2) між підозрюваним та свідками	**1**
	3) між підозрюваними особами	**10**
	14.2. Результат одночасного допиту:	
	1) підозрюваний повністю або частково засвідчив свідчення, котрі раніше заперечував	**73**
	2) підозрюваний знову заперечував свідчення	**27**
15	**Залучення спеціаліста до СРД, НСРД та інших процесуальних дій:**	
	1) огляд місця події	**100**
	2) огляд електронної інформації	**100**
	3) обшук	**96**
	4) тимчасовий доступ до речей та документів	**47**

	5) допит	**36**
	6) зняття інформації з транспортних телекомунікаційних мереж та електронних систем	**100**
16	**Експертизи:**	
	16.1. Об'єкти, що направляються на експертизу:	
	1) смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори потерпілого	
	2) смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори підозрюваного	
	3) флеш-накопичувачі	
	4) жорсткі диски	

Додаток Б

Зведені результати опитувань

250 слідчих, 286 працівників оперативних підрозділів, 52 представників кіберполіції, 96 працівників органів прокуратури, 67 працівників експертних установ МВС України

	З а п и т а н н я	**%**
1.	**Вкажіть Ваш вік:**	
	До 25 років	**39**
	25–30 років	**31**
	31–40 років	**25**
	41 рік і старше	**5**
2.	**Вкажіть стаж практичної роботи:**	
	до 1 року	**5**
	від 1 до 3 років	**24**
	від 3 до 5 років	**38**
	від 5 до 10 років	**23**
	понад 10 років	**10**
3.	**Чи мали місце у Вашому підрозділі випадки розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, та чи можете Ви надати інформацію з цього приводу:**	
	так	**100**
	ні	**0**
4.	**Чи розслідували Ви особисто або брали участь у розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу:**	

	так	**58**
	ні	**42**
6.	**Чи вважаєте Ви, що розслідування кримінальних правопорушень зазначеної категорії потребує відповідної кваліфікації уповноваженої особи у цьому напрямі:**	
	так	**96**
	ні	**4**
7.	**Чи вважаєте Ви необхідним створення окремої комплексної методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу:**	
	так	**92**
	ні	**8**
8.	**Вкажіть, будь ласка, причини низької якості розслідування зазначених діянь:**	
	неналежне процесуальне керівництво досудовим розслідуванням	**56**
	низький фаховий рівень працівників підрозділів правоохоронних органів, які задіяні у кримінальних провадженнях досліджуваної категорії	**62**
	невчасне проведення слідчих (розшукових) дій, НСРД та інших заходів	**32**
	низький рівень координації взаємодії слідчого з працівниками оперативних підрозділів і кіберполіції	**67**
	небажання потерпілих і свідків співпрацювати з уповноваженими особами	**39**
9.	**Які Ви можете назвати тактичні помилки, котрих припускаються слідчі, які розпочали розслідування:**	
	прорахунки у діагностуванні злочинної події та визначенні напрямів розслідування	**84**
	порушення процесуального порядку проведення СРД	**62**

	проведення невідкладних слідчих (розшукових) дій без участі спеціаліста	**57**
	ігнорування встановлення низки важливих обставин	**37**
	«поверхневий» характер невідкладних слідчих (розшукових) дій (огляд, обшук)	**29**
10.	**Вкажіть, будь ласка, найбільш розповсюджені форми взаємодії при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу:**	
	здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів	**91**
	обмін інформацією	**83**
	надання уповноваженій особі відомостей, що зібрані в процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення інформації до ЄРДР	**65**
	групове планування оперативно-розшукових заходів	**31**
	здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, що мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними матеріалами	**29**
11.	**Які типові недоліки у процесі реалізації взаємодії окремих підрозділів під час розслідування кримінальних правопорушень, вчинених із використанням е-банкінгу, Ви можете назвати:**	
	здійснення СРД, НСРД та інших процесуальних дій оперативними працівниками без участі уповноваженої особи	**41**
	невчасний початок здійснення взаємодії	**78**
	спрямування початкових СРД, НСРД та інших процесуальних дій на досягнення «визначальної» мети – затримання	**53**

	правопорушника, в той час як реалізація встановлення обставин вчинення кримінальних правопорушень із використанням е-банкінгу відходить на другий план	
	припинення взаємодії з боку учасників кримінального провадження після закінчення його початкового етапу	**69**
12.	**Які заходи можуть застосовуватися для приховування кримінальних правопорушень, пов'язаних із використанням е-банкінгу:**	
	1) ліквідація устаткування, що застосовувалося для скоєння протиправних дій	**53**
	2) надання завідомо неправдивих показів під час здійснення процесуальних дій (так само як і неправдиве алібі)	**47**
	3) відмова від надання показів	**79**
	4) маскування шпигунського програмного або технічного забезпечення під його законні аналоги	**33**
	5) застосовування зміни ідентифікатора місця знаходження обладнання, за допомогою якого скоєні протиправні дії при застосовуванні е-банкінгу	**64**
13.	**Чи виникають під час допиту підозрюваного в досліджуваній категорії кримінальних проваджень конфліктні ситуації:**	
	так	**79**
	ні	**21**
14.	**Назвіть, будь ласка, ситуації, що виникали під час проведення допиту підозрюваного при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу:**	
	підозрюваний повідомляє інформацію про обставини протиправного діяння, однак не висвітлює її у повному обсязі, що відбувається через:	**27**
	– страх помсти з боку співучасників	**48**
	– залежність від його організатора	**19**
	– заінтересованість у результатах провадження	**33**
	підозрюваний не бажає давати повні та щирі показання – факт конфліктної ситуації	**35**

	підозрюваний цілком відмовляється від комунікації з уповноваженою особою, відмовляється давати показання, а також брати участь у проведенні окремих СРД	**34**
	підозрюваний не заперечує факт і зміст протиправного діяння, однак спростовує свою участь у його вчиненні	**4**
15.	**Назвіть, будь ласка, головні форми використання спеціальних знань під час розслідування досліджуваної категорії протиправних діянь:**	
	консультативно-довідкова допомога	**41**
	участь спеціаліста у проведенні СРД, НСРД	**74**
	призначення експертиз	**100**
	інше	**22**

Додаток В

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Малютін Е. В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Т. 2. С. 143–147.

2. Малютін Е. В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Т. 2. С. 122–128.

3. Малютін Е. В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 425–428. URL : http://www.lsej.org.ua/9_2021/9_2021.pdf.

4. Малютін Е. В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Держава та регіони. Серія : Право.* 2022. № 2. С. 232–236.

5. Малютін Е. В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

6. Малютін Е. В. Спосіб учинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 77–82.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Малютін Е. В. Обстановка вчинення кримінальних правопорушень, пов’язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134. (публікація тез)

8. Малютін Е. В. Особливості початкового етапу розслідування кримінальних правопорушень, пов’язаних із використанням е-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. 171–173. (публікація тез)

9. Малютін Е. В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 139–141. (публікація тез)

10. Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов’язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146. (публікація тез)

Додаток Г

Акти впровадження результатів дисертаційного дослідження

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор
полковник поліції
Сергій ЧЕРНЯВСЬКИЙ
«26» 02 2024

АКТ

26 02 2024 м. Київ №44/69

Впровадження результатів дисертації Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі: начальника відділу організації наукової діяльності та захисту прав інтелектуальної власності, підполковника поліції **В.В. Корольчука,** т.в.о. начальника відділу докторантури та ад'юнктури **А.П. Містюка,** завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента, капітана поліції **А.О. Антонюка,** завідувача загальної бібліотеки **Л.Г. Гайдар**.

Комісія розглянула й узагальнила результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права **Малютіна Едуарда Вікторовича** на тему: «**Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу**» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Проаналізовано основні результати дослідження Е.В. Малютіна, зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Малютін Е.В. Наукові дискусії щодо кримінальних правопорушень, пов'язаних із використанням е-банкінгу, та побудови їх криміналістичної

характеристики. *Актуальні проблеми криміналістичного забезпечення досудового розслідування*: матеріали наук.-практ. семінару (м. Дніпро, 25 трав. 2018 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. С. 152–154.

2. Малютін Е.В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Том 2. С. 143–147.

3. Малютін Е.В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Том 2. С. 122–128.

4. Малютін Е.В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 456–460.

5. Малютін Е.В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія: Право*. 2022. № 2. С. 232–236.

6. Малютін Е.В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183. (Республіка Польща).

7. Малютін Е.В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного*. 2024. Випуск 2. С. 77–82.

8. Малютін Е.В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

9. Малютін Е.В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

10. Малютін Е.В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 139–141.

11. Малютін Е.В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня

2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146.

На основі проведеного аналізу комісія зробила висновок, що праці Е.В. Малютіна містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в науковій діяльності Національної академії внутрішніх справ, зокрема через проведення подальших наукових досліджень з проблем криміналістики, підготовку наукових робіт, видання монографії за результатами наукової роботи.

Члени комісії: **Віктор КОРОЛЬЧУК**

Андрій МІСТЮК

Андрій АНТОЩУК

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор
Харківського національного
університету внутрішніх справ
заслужений юрист України
доктор юридичних наук, професор

Олександр МУЗИЧУК

«29» 02 2024 року

АКТ
впровадження у науково-дослідну діяльність
Харківського національного університету внутрішніх справ результатів дисертаційного дослідження Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-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: професора кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ, доктора юридичних наук, професора Степанюка Р.Л.

членів комісії: професора кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктора юридичних наук, професора Юхна О.О.

начальника відділу організації наукової діяльності та захисту інтелектуальної власності Харківського національного університету внутрішніх справ, кандидата юридичних наук, доцента Абламського С.Є.

склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-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 Малютіна Е.В. використовуються у науково-дослідницькій роботі Харківського національного університету внутрішніх справ з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень у кіберсфері.

Основні результати дисертації відображено у наступних наукових

публікаціях здобувача, зокрема:

Малютін Е.В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Том 2. С. 143–147.

Малютін Е.В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Том 2. С. 122–128.

Малютін Е.В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 456–460.

Малютін Е.В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія: Право*. 2022. № 2. С. 232–236.

Малютін Е.В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge. Education. Law. Management*. 2023. № 3. С. 178–183. (Республіка Польща).

Малютін Е.В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

Малютін Е.В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

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 «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу»; актуальність, вчасність і практичну значущість дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України. Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а

також були враховані профільними кафедрами Харківського національного університету внутрішніх справ при проведенні наукових досліджень.

Голова комісії:

професор кафедри оперативно-розшукової діяльності та розкриття злочинів Харківського національного університету внутрішніх справ доктор юридичних наук, професор — **Руслан СТЕПАНЮК**

Члени комісії:

професор кафедри криміналістики, судової експертології та домедичної підготовки Харківського національного університету внутрішніх справ доктор юридичних наук, професор — **Олександр ЮХНО**

начальник відділу організації наукової діяльності та захисту інтелектуальної власності Харківського національного університету внутрішніх справ, кандидат юридичних наук, доцент — **Сергій АБЛАМСЬКИЙ**

ЗАТВЕРДЖУЮ
Проректор
Дніпровського державного
університету внутрішніх справ
доктор юридичних наук, професор,
Заслужений діяч науки і техніки України
полковник поліції

Олександр ЮНІН

«__» _____ 2024 року

АКТ
впровадження у наукову діяльність
Дніпровського державного університету внутрішніх справ
результатів дисертаційного дослідження

Про впровадження у наукову діяльність Дніпровського державного університету внутрішніх справ результатів дисертаційного дослідження Малютіна Е.В. «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голова комісії: т.в.о. начальника відділу організації наукової роботи Дніпровського державного університету внутрішніх справ, кандидата історичних наук, доцента Прошина Д.В.

члени комісії: заступника директора ННІ права та підготовки фахівців для підрозділів Національної поліції Дніпровського державного університету внутрішніх справ, доктора юридичних наук, доцента Обшалова С.В.

професора кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ, доктора юридичних наук, професора Пирога І.В.

професора кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ, доктора юридичних наук, професора Єфімова М.М.

відповідно до Пріоритетних напрямів наукових досліджень Дніпровського державного університету внутрішніх справ на 2023-2024 навчальний рік склала цей акт з приводу того, що комісією розглянуто результати дисертаційного

дослідження здобувача Науково-дослідного інституту публічного права Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Основні результати дослідження використовуються у НДІДКР Дніпровського державного університету внутрішніх справ для подальшої розробки проблемних питань методики розслідування кримінальних правопорушень у сфері економіки. Результати дисертації відображено у наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (статтях і тезах доповідей на конференціях):

Малютін Е.В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Том 2. С. 122–128.

Малютін Е.В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 456–460.

Малютін Е.В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія: Право*. 2022. № 2. С. 232–236.

Малютін Е.В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183. (Республіка Польща).

Малютін Е.В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного*. 2024. Випуск 2. С. 77–82.

Малютін Е.В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

Малютін Е.В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

На основі проведеного аналізу комісія зробила висновок, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, відповідність спеціальності 12.00.09 та планам НДіДКР ДДУВС на 2023-2024 н.р., а також були враховані профільними кафедрами Дніпровського державного університету внутрішніх справ при проведенні науково-практичних заходів з актуальних питань застосування кримінального процесуального законодавства, проблем протидії економічній злочинності та методики розслідування окремих видів кримінальних правопорушень, а також наукових досліджень на замовлення Головного Управління Національної поліції в Дніпропетровській області.

Голова комісії: **Денис ПРОШИН**

Члени комісії: **Сергій ОБШАЛОВ**

Ігор ПИРІГ

Микола ЄФІМОВ

ЗАТВЕРДЖУЮ
Перший проректор
Національної академії
внутрішніх справ
доктор юридичних наук, професор
полковник поліції

Станіслав ГУСАРЄВ

_____ 2024

АКТ

12 01 2024 м. Київ № 13/24

Впровадження результатів дисертації Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі: т.в.о. начальника навчально-методичного відділу НАВС, лейтенанта поліції **В.О. Бойчук**, начальника відділу організації наукової діяльності та захисту прав інтелектуальної власності, підполковника поліції **В.В. Корольчука,** т.в.о. начальника відділу докторантури та ад'юнктури **А.П. Містюка,** завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента, капітана поліції **А.О. Антощука,** завідувача загальної бібліотеки **Л.Г. Гайдар**.

Комісія розглянула й узагальнила результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права **Малютіна Едуарда Вікторовича** на тему: «**Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу**» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-

розшукова діяльність.

Проаналізовано основні результати дослідження Е.В. Малютіна, зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Малютін Е.В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Том 2. С. 143–147.

2. Малютін Е.В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Том 2. С. 122–128.

3. Малютін Е.В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 456–460.

4. Малютін Е.В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія: Право*. 2022. № 2. С. 232–236.

5. Малютін Е.В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

6. Малютін Е.В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного*. 2024. Випуск 2. С. 77–82.

7. Малютін Е.В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

8. Малютін Е.В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

На основі проведеного аналізу комісія зробила висновок, що праці **Е.В. Малютіна** містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому

процесі Національної академії внутрішніх справ, зокрема при викладанні навчальних дисциплін «Криміналістика», «Криміналістичне забезпечення досудового розслідування», «Інновації у криміналістиці» та ін., під час підготовки навчально-методичних і дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

Вікторія БОЙЧУК

Віктор КОРОЛЬЧУК

Андрій МІСТЮК

Андрій АНТОЩУК

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Директор інституту права
та суспільних відносин
Відкритого міжнародного
університету розвитку людини
«Україна»

Тетяна ФЕДОРЕНКО

«15» 03 2024 року

АКТ

Про впровадження в освітній процес та наукову діяльність Інституту права та суспільних відносин «Відкритого міжнародного університету розвитку людини «Україна» основних результатів дисертації Малютіна Едуарда Вікторовича «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Укладена комісія у складі:

Голови: заступника директора інституту права та суспільних відносин університету «Україна», кандидата юридичних наук, доцента Ізуїта П.О.

Членів комісії: завідувача кафедри галузевого права та загальноправових дисциплін інституту права та суспільних відносин університету «Україна» Фаста О.О.
доцента кафедри кафедри галузевого права та загальноправових дисциплін інституту права та суспільних відносин університету «Україна» Сердюка В.П.

Комісія склала цей акт з приводу того, що було розглянуто результати дисертаційного дослідження «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність, яке підготував здобувач Науково-дослідного інституту публічного права Малютін Едуард Вікторович, у вигляді наукових статей і тез доповідей на науково-практичних конференціях та семінарах.

На підставі наукового дослідження підготовлено наукові статті та тези доповідей, зокрема:

Малютін Е.В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Том 2. С. 143–147.

Малютін Е.В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Том 2. С. 122–128.

Малютін Е.В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 456–460.

Малютін Е.В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія: Право*. 2022. № 2. С. 232–236.

Малютін Е.В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

Малютін Е.В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного*. 2024. Випуск 2. С. 77–82.

Малютін Е.В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *Виклики сучасності та наукові підходи до їх вирішення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 12–13 серпня 2020 р.). Київ : Наук.-дослід. ін-т публічного права, 2020. С. 132–134.

Малютін Е.В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

Малютін Е.В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 139–141.

Малютін Е.В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість для науки кримінального процесу, криміналістики та оперативно-розшукової діяльності, а також були враховані відділом організації наукової роботи та навчально-методичним відділом Інституту права та суспільних відносин «Відкритого міжнародного університету розвитку людини «Україна» при проведенні навчальних занять та наукових досліджень.

Голова комісії: **Петро ІЗУЇТА**

Члени комісії: **Олексій ФАСТ**

Василь СЕРДЮК

ЗАТВЕРДЖУЮ
Начальник УСР
в Дніпропетровській області
ДСР НП України
полковник поліції

Віктор ДІДЕНКО

«27» 09 2023

АКТ
впровадження у практичну діяльність Управління стратегічних розслідувань в Дніпропетровській області ДСР Національної поліції України результатів дисертаційного дослідження Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала комісія у складі:

голови: начальник 9-го відділу (моніторингу та координації) УСР в Дніпропетровській області ДСР НП України, підполковник поліції, кандидат юридичних наук А.В. Макашов

члени комісії: начальник 8-го відділу (інформаційно-аналітичного забезпечення) УСР в Дніпропетровській області ДСР НП України, майор поліції Д.С. Приходько

старший оперуповноважений 4-го відділу (протидії ОЗГ в органах державної влади) УСР в Дніпропетровській області ДСР НП України, майор поліції П.А. Петраш

старший оперуповноважений 5-го відділу (боротьби з ОЗГ з ознаками корупції) УРВ в Дніпропетровській області ДСР НП України, майор поліції Д.М. Мирошниченко

Комісія відповідно до Положення про організацію проведення науково-дослідних та дослідно-конструкторських робіт у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15 травня 2007 року № 154 склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Малютіна Едуарда Вікторовича на тему: «Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 (кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність) у вигляді

розшукова діяльність) у вигляді фахових наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

Малютін Е.В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Том 2. С. 143–147.

Малютін Е.В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Том 2. С. 122–128.

Малютін Е.В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 456–460.

Малютін Е.В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія: Право*. 2022. № 2. С. 232–236.

Малютін Е.В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183. (Республіка Польща).

Малютін Е.В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *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. 132–134.

Малютін Е.В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-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. 171–173.

Малютін Е.В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики : матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 139–141.

Малютін Е.В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства : матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 144–146.

Комісія вважає, що представлені матеріали дисертаційного дослідження, фахові наукові статті та тези доповідей, отримані на основі проведеного інноваційного наукового дослідження, мають необхідний теоретичний і методологічний рівень й практичну значущість та можуть бути впроваджені у діяльність Управління стратегічних розслідувань в Дніпропетровській області ДСР НП України.

Голова комісії: **Антон МАКАШОВ**

Члени комісії: **Данило ПРИХОДЬКО**

Павло ПЕТРАШ

Дмитро МИРОШНИЧЕНКО