МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

КОВАЛЕНКО ІЛЛЯ ОЛЕКСАНДРОВИЧ

УДК 343.98: 343.131

РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

081 Право

08 Право

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **І. О. Коваленко**

Науковий керівник – **Єфімов Микола Миколайович**,
доктор юридичних наук, доцент

Дніпро – 2022

АНОТАЦІЯ

Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – Право. – Дніпропетровський державний університет внутрішніх справ. Дніпро, 2022.

У дисертації вперше на монографічному рівні комплексно досліджено особливості розслідування шахрайства у сфері використання банківських електронних платежів.

Визначено структуру криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів, що має такі елементи: спосіб учинення шахрайства, обстановка вчинення кримінального правопорушення, слідова картина, особа шахрая та особа потерпілого. Встановлено, що вказані складові мають сталі кореляційні зв’язки та важливе значення для початкового етапу кримінального провадження з огляду на можливість висунення відповідних версій, а також проведення певних слідчих та негласних слідчих (розшукових) дій.

Систематизовано способи вчинення зазначеного протиправного діяння, базуючись на тому, що така складова містить підготовку, безпосереднє вчинення та приховування протиправного діяння. Серед найбільш розповсюджених способів безпосереднього вчинення досліджуваного виду шахрайства у процесі користуванні онлайн-банкінгом, мобільним зв’язком, послугами Інтернет-магазинів, визначено фішинг, сніфферінг, вішинг, кардинг. Визначено способи підготовки та приховування кримінального правопорушення.

З’ясовано зміст обстановки та слідової картини вчинення шахрайства у сфері використання банківських електронних платежів. Зокрема, у процесі вчинення такого шахрайства дії шахраїв можуть складатися із ряду операцій,

пов’язаних із втручанням до облікових записів, електронних скриньок та інших електронних ресурсів користувачів мережі Інтернет, що тривають у часі та здійснюються на необмеженій території. У зв’язку із чим набуває актуальності встановлення часово-просторових характеристик вчинення шахрайських дій. Часові параметри є достатньо розпливчастими, утім часом вчинення шахрайства у сфері електронних банківських платежів слід враховувати момент проведення транзакції, завдяки якій потерпілого було позбавлено грошей на його рахунку.

У фізичному сенсі місцями вчинення шахрайства у сфері банківських електронних платежів можуть бути: місця знаходження комп’ютерної техніки, за допомогою якої здійснюються шахрайські дії (стаціонарне комп’ютерне обладнання, ноутбук (телефон, планшет), що переміщується у просторі і підключений до мережі Інтернет) – 78 %; місця знаходження банкоматів, банків, в яких знімалася готівка – 56 %; місце знаходження потерпілого, який виявив шахрайські дії при здійсненні електронних платежів – 67 % тощо. Утім, умови вчинення такого шахрайства слід розглядати і як віртуальний простір, у якому передається, зчитується та змінюється електронно-цифрова інформація, завдяки якій здійснюється втручання до облікових записів користувачів мережі Інтернет та знімаються грошові суми внаслідок незаконних транзакцій.

До складу обстановки вчинення шахрайства у сфері використання банківських платежів запропоновано віднести й систему інформаційних ресурсів, пов’язаних із функціонуванням платіжних систем, через які проводяться транзакції та рівень інформаційної безпеки у банківській сфері.

Слідова картина шахрайств у сфері електронних банківських платежів включає 3 групи слідів: 1) матеріальні сліди, що відображаються у квитанціях та роздруківках про електронні банківські платежі (68 %); на банківських картках (46 %); на сім-картках (37 %); на паперових копіях комп’ютерної інформації (44 %); сліди папілярних ліній на засобах комп’ютерної техніки, клавіатурі терміналу (17 %) тощо; 2) ідеальні сліди,

що складають 28 % і відображаються у пам'яті потерпілих та осіб, які були свідками незаконних операцій із банківськими платежами з боку шахраїв; 3) віртуальні сліди (електронно-цифрові), що займають домінуюче місце і містяться: у пам'яті мобільного телефону (IMEI-код; історія телефонних з'єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо) – 88 %; на сервері мобільного оператора – 76 %; на сервері інтернет-провайдера (сервер зберігання flow-статистики и биллінгової інформації, сервер баз даних тощо) – 67 %; в пам'яті сім-карти – 79 %; у пам'яті комп'ютерів, планшетів – 92 %; у електронній поштовій скриньці – 56 %; на флеш карті (файли, папки тощо) – 34 %; дані електронного журналу банкомату (терміналу) – 29 %; інформація в електронному вигляді, що відображає суми грошових коштів, переказаних через певну систему електронних платежів («Приват-банк», «Qiwi-гаманець», MoneyGram, Western Union, Perfect Money та ін.) – 48 %; профіль у соціальних мережах, інформація на сайтах – 42 % тощо.

Встановлено криміналістично вагомі ознаки особи шахрая, а також складено його типовий портрет. Так, було визначено, що шахрайства в сфері 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.

Виокремлено віктимогенні групи потерпілих, а саме: 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

Сформовано систему обставин, що підлягають встановленню у кримінальному провадженні за фактами вчинення шахрайства у сфері

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

Сформульовано типові слідчі ситуації розслідування досліджуваного виду шахрайства, зокрема: 1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація,

шахрай відомий – 19 %; 2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %; 3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %; 4) вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %.

Виокремлено організаційно-тактичні аспекти проведення окремих СРД, спрямованих на отримання інформації з матеріальних та особистісних джерел. Зазначено, що шахрайства у сфері використання електронних банківських платежів переважно здійснюються за допомогою спеціальних програм, що маскують реальне місце знаходження особи шахрая так званих анонімайзерів таких як VPN – скорочена назва від англ. Virtual Privat Network – віртуальна приват мережа, Socks скорочена назва від англ. Socked Secure – мережевий протокол та ін. Здебільшого такі протиправні діяння вчиняються або ОГ, або ЗО. Визначено категорії свідків у процесі розслідування досліджуваної категорії протиправних діянь, а саме: особи, яким може бути відома інформація про обставини та умови протиправної діяльності, що вони спостерігали; особи, які перебувають у родинному або іншому зв’язку із шахраєм; особи, яким відомо умови та обставини тих дій, у яких вони брали участь; особи, які певним чином сприяли вчиненню шахрайства, але самі про це не знали; особи, які були обізнані про обставини, що передували шахрайству; працівників банківських установ, які були задіяні в використанні банківських електронних платежів.

Встановлено, що підозрюваному у вчиненні шахрайства у сфері використання банківських електронних платежів потрібно ставити певні категорії питань: за яких обставин вчинено шахрайські дії; що за способи застосовувалися (використання ботів для спаму та потрапляння шкідливих програм до комп’ютерного забезпечення потерпілого; використання

реквізитів картки, що є викраденими з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, із персональних комп'ютерів користувачів); які місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); засоби, що використовувалися під час скоєння правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації); яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчинення протиправних дій; що за порядок розподілу грошових коштів був у членів ОГ чи ЗО; протягом якого періоду вчинялись протиправні діяння; які супутні кримінальні правопорушення було вчинено.

Охарактеризовано організаційно-тактичні особливості проведення обшуку та огляду. Зокрема, вказано, що обшук переважно проводився в місцях: зберігання й обробки інформації про банківські електроні платежі, що зазнала злочинного впливу (67 %); знаходження комп'ютерного обладнання, що використовувалося у процесі здійснення протиправного діяння (43 %); збереження інформації, отриманої злочинним шляхом (41 %); настання шкідливих наслідків (10 %). Під час огляду електронних інформаційних систем (комп'ютер, планшет, мобільний телефон, тощо) об'єктом огляду є така техніка, а також носії інформації (наприклад, IP-адреси, системні дані, програми, cookies браузерів, КЕШ та ін.).

З'ясовано організацію і тактику проведення окремих НСРД при розслідуванні шахрайства у сфері банківських електронних платежів. На основі вивчення матеріалів кримінальних проваджень було встановлено, що специфічною ознакою досліджуваної категорії протиправних діянь є потреба проведення цілого ряду НСРД та оперативно-технічних заходів, пов'язаних із встановленням шахрая та його зв'язків. Зокрема, серед них було виокремлено

такі як спостереження за об’єктом, огляд кореспонденції, прослуховування телефонних переговорів, зняття інформації з транспортних та електронних систем. Зазначено, що реалізація НСРД відповідно до процесуального порядку є неодмінною умовою того, щоб їх результати здійснення суд вбачав допустимими.

Конкретизовано особливості призначення експертиз у кримінальних провадженнях вказаної категорії. Зокрема, під час проведення підвиду СКТЕ експерту потрібно зупинитися на таких моментах: виявити відношення досліджуваної техніки до апаратних комп’ютерних засобів; визначити тип, марку або модель даного пристрою; встановити технічні характеристики і параметри досліджуваного технічного засобу; визначити первинну конфігурацію і характеристики даного пристрою, а також дізнатись, чи були змінені його функціональні властивості, порівняно з первісною конфігурацією; провести зовнішній огляд техніки з метою виявлення фізичного втручання до його конфігурації; встановити, чи є цей технічний засіб накопичувачем інформації, та чи відкритий доступ до такої інформації.

Практичне значення одержаних результатів полягає у тому, що розроблені у дисертації положення та рекомендації можуть бути використані та використовуються у: *науковій діяльності* – для подальшого поліпшення окремих аспектів методики розслідування кримінальних правопорушень на базі сформульованих та означених теоретичних положень, висновків та рекомендацій (акт впровадження Дніпропетровського державного університету внутрішніх справ від 20.11.2021 р.); *освітньому процесі* – під час викладання навчальних дисциплін «Криміналістика», «Кримінальний процес», «Криміналістичні засоби та методи розслідування кримінальних правопорушень», «Організація розслідування кримінальних правопорушень», «Оперативно-розшукова діяльність», а також під час підготовки підручників, посібників, текстів лекцій і навчально-методичних матеріалів, проведенні семінарів і практичних занять із кримінального процесу, криміналістики та оперативно-розшукової діяльності (акти впровадження Дніпропетровського

державного університету внутрішніх справ від 11.11.2021 р.); *практичній діяльності* – для вдосконалення діяльності правоохоронних органів під час розслідування кримінальних правопорушень проти власності (акти впровадження Дніпропетровського НДЕКЦ МВС від 14.04.2020 р., Управління стратегічних розслідувань у Дніпропетровській області ДСР Національної поліції України від 11.05.2021 р.).

Ключові слова: *шахрайство, банківські електронні платежі, фішинг, кардинг, криміналістична характеристика, досудове розслідування, слідча ситуація, слідча (розшукова) дія, негласна слідча (розшукова) дія, експертиза.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації:

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

2. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

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

4. 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.

5. Коваленко І. О. Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник.* 2021. № 1 (36). С. 98–101.

Наукові праці, що засвідчують апробацію матеріалів дисертації:

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

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

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

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

10. Коваленко І. О. Окремі питання визначення обставин, що

підлягають встановленню при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Актуальні проблеми криміналістики та судової експертизи*: матеріали наук.-практ. семінару (м. Дніпро, 28 трав. 2021 р.). Дніпро : ДДУВС, 2021. С. 145–147.

ANNOTATION

Kovalenko I. O. Fraud investigation in the use of bank electronic payment transactions. – Qualifying scientific work on manuscript rights.

Dissertation for the degree of doctor of philosophy (PhD) in specialty 081– Law. Dnipropetrovsk State University of Internal Affairs. Dnipro, 2022.

The specifics of fraud investigation in the use of bank electronic payment transactions are comprehensively researched in the dissertation for the first time monographically.

The structure of the forensic characteristics of fraud in the use of bank electronic payment transactions is defined, which includes the following elements: the method of committing fraud, the circumstances of the commission of a criminal offense, the trace pattern, the identity of the fraudster and the identity of the victim. It has been established that the specified components have constant correlations and are important for the initial stage of criminal proceedings, given the possibility of putting forward relevant versions, as well as carrying out a number of investigative and covert investigative (search) actions.

The methods of committing the specified illegal act are systematized based on the fact that this component includes preparation, direct commission and concealment of the illegal act. Phishing, sniffing, vishing, and carding are among the most common ways of directly committing the investigated type of fraud when using online banking, mobile communications, and services in online stores. Methods of preparation and concealment of a criminal offense are defined.

The content of the situation and the trace pattern of committing fraud in the use of bank electronic payment transactions have been clarified. In particular, when committing such fraud, the actions of fraudsters may consist of a number of operations related to interference with accounts, electronic mailboxes and other electronic resources of Internet users, which last over time and are carried out in an unlimited territory. In connection with this, establishing the temporal and spatial characteristics of committing fraudulent acts becomes relevant. The time parameters are rather vague, however, the time of committing fraud in the field of electronic bank payments should be considered the moment of the transaction, thanks to which the victim was deprived of money from his account.

In the physical sense, places where fraud in the field of electronic banking payments is committed can be: locations of computer equipment from which fraudulent actions are carried out (stationary computer equipment, laptop (phone, tablet), which moves in space and is connected to the Internet) – 78 %; locations of ATMs, banks where cash was withdrawn – 56 %; the location of the victim who detected fraudulent actions when making electronic payments – 67 %, etc. However, the environment for committing this fraud should also be considered as a virtual space in which electronic and digital information is transmitted, read and changed, thanks to which the accounts of Internet users are interfered with and money is withdrawn as a result of illegal transactions.

The system of information resources related to the functioning of payment systems through which transactions are carried out and the level of information security in the banking sector are proposed to be included in the composition of the situation of committing fraud in the use of bank electronic payment transactions.

The trace pattern of fraud in the field of electronic bank payments includes 3 groups of traces: 1) material traces displayed in receipts and printouts of electronic bank payments (68 %); on bank cards (46 %); on SIM cards (37 %); on paper copies of computer information (44 %); traces of papillary lines on computer equipment, terminal keyboard (17 %), etc.; 2) perfect traces, which make up 28 % and are reflected in the memory of victims and persons who witnessed illegal

operations with bank payments by fraudsters; 3) virtual traces (electronic-digital), which occupy a dominant place and are contained: in the memory of the mobile phone (IMEI code; history of telephone connections, history of voice messages; history of text messages; software for conducting banking operations from the phone etc.) – 88 %; on the server of the mobile operator – 76 %; on the Internet provider's server (flow statistics and billing information storage server, database server, etc.) – 67 %; in the SIM card memory – 79 %; in the memory of computers, tablets – 92 %; in an electronic mailbox – 56 %; on a flash card (files, folders, etc.) – 34 %; ATM (terminal) electronic log data – 29 %; information in electronic form that reflects the sums of funds transferred through a certain electronic payment system ("Privat-bank", "Qiwi-wallet", MoneyGram, Western Union, Perfect Money, etc.) – 48 %; profile in social networks, information on websites – 42 %, etc.

Forensically significant signs of the fraudster's identity were found, and his typical portrait was drawn up. Thus, it was determined that fraud in the use of bank electronic payment transactions is mainly committed by male persons aged 25-35, who have a higher education, are single and work in the field of entrepreneurial activity and the field of computer technologies.

Victimogenic groups of victims are singled out: a) persons who were influenced by acquaintances and relatives during the implementation of bank electronic payments; b) persons who were deceived by strangers during the implementation of bank electronic payments; c) persons who disclosed their personal data to employees of the banking sector; d) persons who, due to negative mental states, were exposed to the influence of strangers during the implementation of bank electronic payments.

A system of circumstances that must be detected in criminal proceedings based on the facts of fraud in the field of using bank electronic payments has been formed, in particular, the following are defined among them: 1) circumstances that characterize the commission of fraud in the use of bank electronic payment transactions (information about the time and place of the fraud, information about

the method of its commission, for example: the use of bots for spam and the introduction of malicious programs into the computer support of the victim; the use of card details that are stolen from the servers of e-commerce stores, payment and settlement systems, from personal computers of users; information about traces of an illegal act, determining the place of obtaining illegal access and integration into the network (from the inside or outside) and ways of making an illegal connection (hacking of data protection programs, manipulation of data, commands and information, use of fraudulent programs, technical techniques); means used in committing a crime: these can be both technical, such as EOT, smartphones, tablets, modems, routers, and software, such as VPN, browsers, graphic editors, information encoding programs); 2) circumstances relating to the characteristics of the criminal and the victim (the number of offenders – the fact of distribution of functions among the fraudsters, the tasks of each of them); 3) cause-and-effect relationships: the presence of a certain relationship between the actions of guilty persons and their results; clarification of the reasons and conditions that contributed to the commission of an illegal act; 4) circumstances that aggravate, mitigate the punishment or generally exclude criminal responsibility (whether there are conditions and grounds for closing criminal proceedings); 5) qualifying signs regarding the amount of damage caused by the illegal act and the circumstances that are grounds for exemption from criminal liability; 6) the type and amount of damage caused by fraud in the use of bank electronic payment transactions.

Typical investigative situations of inquiry the researched type of fraud are formulated: 1) fraud was committed in the field of using bank electronic payments, personal evidentiary information is available, the fraudster is known – 19 %; 2) fraud was committed in the field of using bank electronic payments, personal evidence is available, the fraudster is unknown – 47 %; 3) fraud has been committed in the field of using bank electronic payments, material and personal evidence is available, the fraudster is known, but his actions are disguised as legitimate financial transactions – 11 %; 4) fraud has been committed in the field

of using bank electronic payments, there is a statement from the victim, there is no sufficient evidentiary information – 23 %.

The organizational and tactical aspects of conducting separate SRD aimed at obtaining information from material and personal sources are highlighted. It is noted that frauds in the field of using electronic bank payments are usually carried out with the help of special programs that mask the real location of the fraudster's identity, so-called anonymizers such as VPN– a virtual private network, Socks is an abbreviated name Socketed Secure – network protocol, etc. For the most part, such illegal acts are committed either by OG or ZO. The categories of witnesses during the investigation of the researched category of illegal acts are defined: persons who may know information about the circumstances and conditions of the illegal activity they observed; persons who are in a family or other relationship with the fraudster; persons who know the conditions and circumstances of the actions in which they participated; persons who in a certain way contributed to the commission of fraud, but did not know about it; persons who were aware of the circumstances preceding the fraud; employees of banking institutions who were involved in the use of bank electronic payments.

It has been found that certain questions of the following category must be asked to the person suspected of committing fraud in the use of bank electronic payment transactions: for which fraudulent actions were essentially committed; what methods are used (use of bots for spam and use of malicious programs for the computer support of the victim; use of card details that are stolen from the servers of e-commerce stores, payment and settlement systems, from personal computers of users); what are the places of gaining illegal access and integration into the network (from inside or outside) and ways of committing illegal connection (hacking of data protection programs, manipulation of data, commands and knowledge, use of fraudulent programs, technical techniques); what means were used when committing the offense: these can be both technical, such as ECM, smartphones, tablets, modems, routers, and software, such as VPN, browsers, graphic editors, information encoding programs; what is the total amount of

material values or monetary funds formed as a result of committing illegal actions; what was the procedure for distributing funds to members of the OG or ZO; during which period the illegal actions were committed; what related criminal offenses were committed.

The organizational and tactical features of the search and inspection are characterized. In particular, it was indicated that in most cases the search was carried out in the following places: storage and processing of information about bank electronic payments, which was subject to criminal influence (67 %); finding computer equipment used in the commission of an illegal act (43 %); preservation of information obtained by criminal means (41 %); occurrence of harmful consequences (10 %). When inspecting electronic information systems (computer, tablet, mobile phone, etc.), the object of inspection is such equipment, as well as information carriers (for example, IP addresses, system data, programs, browser cookies, cache, etc.).

The organization and tactics of carrying out separate investigation actions in the investigation of fraud in the use of bank electronic payment transactions have been clarified. Based on the study of the materials of criminal proceedings, it was found that a specific feature of the investigated category of illegal acts is the need to carry out a number of investigation actions and operational and technical measures related to the establishment of the fraudster and his connections. In particular, among them, the following were singled out: monitoring the object, reviewing correspondence, listening to telephone conversations, and removing information from transport and electronic systems. It is indicated that the implementation of investigation actions in accordance with the procedural order is an indispensable condition for the results of their implementation to be considered admissible by the court.

The specifics of the assignment of expert examinations in criminal proceedings of the specified category have been concretized. In particular, when conducting a subspecies of investigation actions, the expert must focus on the following points: identify the relationship of the researched equipment to computer

hardware; determine the type, brand or model of this device; establish the technical characteristics and parameters of the technical means under investigation; determine the initial configuration and characteristics of this device, as well as find out whether its functional properties have been changed, compared to the initial configuration; conduct an external inspection of the equipment for physical interference in its configuration; establish whether this technical means is an information storage device and whether access to such information is open.

The practical significance of the obtained results is that the provisions and recommendations developed in the dissertation can be used and are used in: *scientific activity* – for the further improvement of certain aspects of the methodology of the investigation of criminal offenses on the basis of formulated and defined theoretical provisions, conclusions and recommendations (act of implementation of the Dnipropetrovsk State University of Internal Affairs from November 20, 2021); *educational process* – during the teaching of the educational disciplines "Forensics", "Criminal process", "Forensic means and methods of investigation of criminal offenses", "Organization of the investigation of criminal offenses", "Operational investigative activity", as well as during the preparation of textbooks, manuals, lecture texts and educational and methodological materials, conducting seminars and practical classes on criminal process, criminology and investigative activities (implementing acts of the Dnipropetrovsk State University of Internal Affairs, November 11, 2021); *practical activities* – to improve the activities of law enforcement agencies during the investigation of criminal offenses against property (acts of implementation of the Dnipropetrovsk SRECC of the Ministry of Internal Affairs dated 04.14.2020, the Department of Strategic Investigations in the Dnipropetrovsk Region of the National Police of Ukraine dated 05.11.2021).

Keywords: fraud, bank electronic payments, phishing, carding, forensic characteristics, pre-trial investigation, investigative situation, investigative (search) action, covert investigative (search) action, expertise.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковано основні наукові результати дисертації:

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

2. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

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

4. 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.

5. Коваленко І. О. Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник.* 2021. № 1 (36). С. 98–101.

Наукові праці, що засвідчують апробацію матеріалів дисертації:

6. Коваленко І. О. Деякі аспекти проведення огляду місця події при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Актуальні проблеми забезпечення публічного порядку та безпеки в*

сучасних умовах: вітчизняний та міжнародний досвід: матеріали Міжнар. наук.-практ. конф. (Дніпро, 25 жовт. 2019 р.). Дніпро : ДДУВС, 2019. С. 123–125.

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

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

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

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

ЗМІСТ

Перелік умовних позначень……..22

ВСТУП…….……..23

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ……37

1.1. Ґенеза наукових поглядів щодо криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів.....37

1.2. Криміналістичний аналіз способів вчинення шахрайства у сфері використання банківських електронних платежів.……47

1.3. Обстановка та умови вчинення шахрайства у сфері банківських електронних платежів. Слідова картина ……....62

1.4. Характеристика особи шахрая та потерпілого…….……...79

Висновки до розділу 1……..….95

РОЗДІЛ 2

ОРГАНІЗАЦІЙНІ ЗАСАДИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ……..……...…98

2.1. Аналіз та оцінка початкової інформації, а також коло обставин, що підлягають встановленню…….……...….98

2.2. Типові слідчі ситуації та відповідні їм алгоритми дій працівників правоохоронних органів під час розслідування досліджуваної категорії кримінальних правопорушень…….……...111

Висновки до розділу 2……..…...127

РОЗДІЛ 3

ОСОБЛИВОСТІ ТАКТИКИ ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ……129

3.1. Організація і тактика проведення окремих слідчих (розшукових) дій...129

3.2. Організаційно-тактичні аспекти проведення негласних слідчих (розшукових) дій……..……..…152

3.3. Особливості призначення експертиз у кримінальних провадженнях досліджуваної категорії……..……..……162

Висновки до розділу 3……..……...174

ВИСНОВКИ…….……..176

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….……..183

ДОДАТКИ…….……..208

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АКЕ	–	Апаратно-комп’ютерна експертиза
ГУНП	–	Головне управління Національної поліції
ЕОМ	–	Електронно-обчислювальна машина
ЕОТ	–	Електронно-обчислювальна техніка
ЕПС	–	Електронно-платіжні системи
ЄРДР	–	Єдиний реєстр досудових розслідувань
ЗО	–	Злочинні організації
ІКЕ	–	Інформаційно-комп’ютерна експертиза
КК	–	Кримінальний кодекс
КМЕ	–	Комп’ютерно-мережева експертиза;
КПК	–	Кримінальний процесуальний кодекс
МВС	–	Міністерство внутрішніх справ
НСРД	–	Негласна слідча (розшукова) дія
ОГ	–	Організовані групи
ПКЕ	–	Програмно-комп’ютерна експертиза
ПК	–	Персональний комп’ютер
СКТЕ	–	Судова комп’ютерно-технічна експертиза
СОГ	–	Слідчо-оперативна група
СРД	–	Слідча (розшукова) дія
ЦК	–	Цивільний кодекс України
ЦПК	–	Цивільний процесуальний кодекс України
п.	–	Пункт
р.	–	Рік
с.	–	Сторінка (сторінки)
ст.	–	Стаття
ч.	–	Частина

ВСТУП

Обґрунтування вибору теми дослідження. Громадяни мають право володіти, користуватися і розпоряджатися своєю власністю, а також результатами своєї інтелектуальної та творчої діяльності, як передбачено у статті 41 Конституції України. Водночас досить велика кількість протиправних діянь вчинюється саме у сфері власності (крадіжки, грабежі, розбої, шахрайства). Слід наголосити, що протягом останнього десятиліття в Україні та в усьому світі інформаційні технології зробили великий крок уперед, що стало одним із вагомих чинників загострення криміногенної ситуації у сфері банківської діяльності. Адже з масовою комп'ютеризацією та використанням всесвітньої мережі Інтернет діяльність злочинного середовища набула відповідні зміни як серед новітніх способів учинення протиправних діянь, так і серед засобів їх учинення. Окрім того, у зв'язку з розвитком банківської системи України, використанням в банківській діяльності таких продуктів як Internet Banking, Клієнт-Банк та інші збільшилася кількість кримінальних правопорушень у сфері банківських електронних платежів. Із огляду на складність кримінальних проваджень досліджуваної категорії, як у всьому світі, так і в Україні, виникає необхідність у створенні сучасної методики розслідування зазначених протиправних діянь.

Зокрема, відповідно до відомостей Генеральної прокуратури України у 2013 р. було обліковано 3344 фактів шахрайства за ч. 3 ст. 190 Кримінального кодексу України, із яких лише у 983 випадках було складено обвинувальний акт; у 2014 р. було обліковано 2760 вказаних кримінальних правопорушень, із яких обвинувальний акт було складено у 1021 випадку; у 2015 р. – 3656 фактів, з них обвинувальний акт – у 1050 випадках; у 2016 р. – 3611 фактів, із них обвинувальний акт – у 789 випадках; у 2017 р. – 4845 фактів, із них обвинувальний акт – у 1631 випадку; у 2018 р. – 3352 факти, із них

обвинувальний акт – у 845 випадках; у 2019 р. – 2467 фактів, із них обвинувальний акт – у 555 випадках; у 2020 р. було обліковано 14744 факти шахрайства за ч. ч. 2-4 ст. 190 Кримінального кодексу України, із яких у 6412 випадках було складено обвинувальний акт; за 10 місяців 2021 року було обліковано 13193 визначених кримінальних правопорушення, із яких обвинувальний акт було складено лише у 5496 випадку.

Відтак, майже кожне кожне третє задокументоване звернення з приводу вчинення досліджуваних протиправних діянь мало наслідком направлення до суду обвинувального акту, тобто 60-70 % залишаються нерозкритими. Окрім того, слід акцентувати увагу на тому, що потерпілими від вчинення різноманітних кримінальних правопорушень (в тому числі і шахрайства) стають працівники банківських установ. Зокрема, у 2016 році ними стало 124 особи, 2017 р. – 92 особи, 2018 р. – 69 осіб, 2019 р. – 49 осіб, 2020 р. – 141 особа, а за 10 місяців 2021 р. – 108 осіб. В той же час, за результати проведеного дослідження серед них випадків вчинення шахрайства у сфері використання банківських електронних платежів становить близько 6 %. Та реально оцінити об’єктивні діапазони вказаних протиправних діянь складно через їх високу латентність, а також делікатну межу між цивільно-правовими та кримінально-правовими відносинами, що обтяжує уповноважених осіб в розрізі прийняття рішення щодо початку кримінального провадження.

Теоретичним базисом для реалізації нашого дослідження стали фундаментальні праці вчених з різних напрямків юридичної науки (криміналістики, кримінального процесу, оперативно-розшукової діяльності, кримінального права, кримінології), котрі внесли змістовний вклад у розробку засад розслідування кримінальних правопорушень, зокрема: Ю. П. Аленіна, Л. І. Аркуші, І. В. Басистої, В. П. Бахіна, В. Д. Берназа, Р. С. Бєлкіна, О. І. Возгріна, А. Ф. Волобуєва, В. І. Галагана, І. Ф. Герасимова, В. Г. Гончаренка, І. В. Гори, О. М. Джужі, Л. Я. Драпкіна, В. Г. Дрозд, В. А. Журавля, В. П. Захарова, А. В. Іщенка, Н. С. Карпова, О. В. Кириченка, А. М. Кислого, Н. І. Клименко, В. А. Колесника, В. П. Колмакова,

В. О. Коновалової, В. П. Корж, В. С. Кузьмічова, В. В. Лисенка, В. К. Лисиченка, Л. М. Лобойка, В. Г. Лукашевича, Є. Д. Лук'янчикова, Г. А. Матусовського, С. І. Мінченка, Д. Й. Никифорчука, О. В. Одерія, В. Л. Ортинського, І. В. Пирога, М. А. Погорецького, М. І. Порубова, О. В. Пчеліної, М. В. Салтевського, Д. Б. Сергєєвої, С. М. Стахівського, Р. Л. Степанюка, А. В. Столітнього, М. П. Стрельбицького, В. Є. Тарасенка, Р. В. Тарасенка, О. Ю. Татарова, В. М. Тертишника, В. В. Тіщенка, В. Г. Уварова, Л. Д. Удалової, І. Ф. Хараберюша, П. В. Цимбала, М. С. Цуцкіридзе, К. О. Чаплинського, С. С. Чернявського, Ю. М. Чорноус, В. В. Шендрика, В. Ю. Шепітька, М. Г. Щербаковського, Б. В. Щура, В. В. Юсупова, О. О. Юхна, М. П. Яблокова та ін.

Значний внесок у дослідження теоретичних питань, пов'язаних з проблемами методики розслідування різних видів шахрайства та окремих його аспектів, зробили такі науковці як А. І. Анапольська, Г. С. Бідняк, О. В. Герасимов, С. В. Головкін, Т. В. Коршикова С. С. Кузьменко, О. В. Курман, В. Р. Мойсик, О. Л. Мусієнко, Н. О. Опанасенко, Т. В. Охрімчук, Н. В. Павлова, В. І. Пазиніч, Д. А. Птушкін, А. В. Реуцький, В. В. Сабадаш, О. А. Самойленко, С. В. Самойлов, Т. .Л. Тропіна, В. Г. Хахановський, К. О. Чередник, С. С. Чернявський, Д. Е. Чувирін, С. В. Чучко та ін.

Серед праць вказаних науковців необхідно виокремити наступні: О.А. Самойленко «Криміналістичне забезпечення розслідування шахрайства з фінансовими ресурсами» (м. Донецьк, 2014), який з'ясував місце шахрайств, учинених із використання мережі «Інтернет», у системі сучасної злочинності; встановив та класифікував способи вчинення означених видів протиправних діянь; виокремив та охарактеризував особливості процесу слідоутворення; дослідив особливості оцінки первинних матеріалів під час прийняття рішення про початок кримінального провадження; дослідив особливості проведення окремих слідчих (розшукових) дій тощо. А вже О. В. Герасимов в своєму дослідженні «Протидія злочинності у банківській

сфері» (м. Харків, 2019) дослідив інституційну злочинність в банківській сфері; визначив елементи кримінологічної характеристики протиправних діянь у банківській сфері; дослідив правові засади та суб'єкти протидії злочинності у вказаній сфері та інше.

Зокрема, О. А. Самойленко у своїй монографії «Основи методики розслідування злочинів, вчинених у кіберпросторі» (м. Одеса, 2020) розглянула кіберпростір та кримінальні правопорушення як об'єкт криміналістичного дослідження; дослідила та визначила структуру криміналістичної характеристики правопорушень, вчинених у кіберпросторі; дослідила особливості відкриття кримінального провадження та взаємодії слідчого під час розслідування протиправних діянь, вчинених у кіберпросторі; охарактеризувала особливості організації розслідування досліджуваної категорії кримінальних правопорушень. Зі свого боку, Т. В. Коршикова у своїй дисертації «Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» (м. Київ, 2021) визначила стан наукових досліджень проблем розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки; розкрила наповнення окремих елементів криміналістичної характеристики досліджуваного виду шахрайства; окреслила обставини, що підлягають встановленню під час розслідування вказаного протиправного діяння; виокремила типові слідчі ситуації та слідчі версії; узагальнила особливості проведення вербальних та невербальних слідчих (розшукових) дій. Наостанок приведемо для прикладу дисертаційне дослідження С. В. Чучко «Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет» (м. Дніпро, 2021), який визначив особливості правового регулювання правовідносин у віртуальному просторі, що впливають на рівень вчинення шахрайства у мережі Інтернет; описав та систематизував типові способи досліджуваного виду шахрайства; розкрив наповнення інших елементів криміналістичної характеристики; виявив проблемні питання початку досудового розслідування вказаного протиправного діяння;

встановив особливості взаємодії різних органів в кримінальних провадженнях досліджуваної категорії; конкретизував організацію і тактику проведення окремих слідчих (розшукових) дій, спрямованих на отримання інформації з матеріальних та особистісних джерел.

Водночас слід наголосити на тому, що наукові праці згаданих науковців, не враховуючи їх вагомість, розкривали лише окремі аспекти розслідування з конкретних видів шахрайства. Окрім того, через ряд змін у законодавстві певні положення або змінилися, або взагалі перестали існувати. Зважаючи на високу латентність шахрайства у сфері використання банківських електронних платежів, виникають суттєві ускладнення у процесі доказування та організаційно-тактичному забезпеченні розслідування вказаних діянь. Це вимагає удосконалення криміналістичних засобів та методів проведення окремих слідчих (розшукових) дій та негласних слідчих (розшукових) дій.

Зазначені чинники сукупно визначили актуальність цієї проблематики, її наукову, теоретичну та практичну значимість, а також зумовили вибір напряму дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертація виконана відповідно до Тематики наукових досліджень та науково-технічних (експериментальних) розробок на 2020-2024 роки, затвердженої наказом МВС України від 11.06.2020 № 454; положень Стратегії сталого розвитку «Україна – 2020» (Указ Президента України № 5/2015); Стратегії національної безпеки України (Указ Президента України № 392/2020); Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1023-р/); Порядку взаємодії Генеральної прокуратури України та МВС України щодо обміну інформацією з ЄРДР та інформаційних систем органів внутрішніх справ (спільний наказ ГПУ та МВС України № 115/1046); Переліку пріоритетних напрямів наукових досліджень в Україні з проблем наук кримінально-правового циклу (рішення Національної академії правових наук України № 3/2019); Пріоритетних напрямів розвитку

правової науки на 2016–2020 роки, що затверджені на загальних зборах Національної академії правових наук України 03.03.2016 р., а також у межах загальноуніверситетської наукової теми Дніпропетровського державного університету внутрішніх справ «Актуальні проблеми кримінально-правового, кримінального процесуального та криміналістичного забезпечення протидії злочинності в Україні» (державний реєстраційний номер 0118U100431).

Мета і завдання дослідження. Метою дослідження є вирішення конкретного наукового завдання щодо розробки методики розслідування шахрайства у сфері використання банківських електронних платежів, а також формулювання на зазначеній основі з урахуванням діючого законодавства науково обґрунтованих пропозицій стосовно удосконалення практики кримінальних проваджень визначеної категорії. Для реалізації окресленої мети сформульовано виконання наступних завдань:

– визначити структуру криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів;

– систематизувати способи вчинення вказаного протиправного діяння;

– з’ясувати зміст обстановки та слідової картини вчинення шахрайства у сфері використання банківських електронних платежів;

– надати характеристику особи шахрая та виокремити віктимогенні групи потерпілих;

– сформувати систему обставин, що підлягають встановленню у кримінальному провадженні;

– сформулювати типові слідчі ситуації та відповідні їм комплекси слідчих (розшукових) дій;

– виокремити організаційно-тактичні аспекти проведення окремих слідчих (розшукових) дій;

– з’ясувати організацію і тактику проведення окремих негласних слідчих (розшукових) дій;

– конкретизував особливості призначення експертиз у кримінальних провадженнях вказаної категорії.

Об'єктом дослідження є кримінально-процесуальні відносини, що виникають під час розслідування шахрайства у питаннях використання банківських електронних платежів.

Предметом дослідження є розслідування шахрайства у сфері використання банківських електронних платежів.

Методи дослідження. Методи дисертаційного дослідження зумовлені специфікою роботи, а також її метою та визначеними завданнями, зважаючи на об'єкт і предмет дослідження. З урахуванням вказаних моментів у дисертації застосовувались загальнонаукові і спеціальні методи наукового пізнання. Основою їх використання фігурував *діалектичний метод*.

Формально-логічні методи застосовувались у процесі аналізу матеріалів кримінальних справ і проваджень, нормативно-правових актів, наукових положень та концепцій, що відображають специфіку дослідження (розділи 1, 2, 3). *Системно-структурний метод* застосовано під час формування системи криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів, а також визначення інформативного наповнення окремих її складових у їх взаємовідношенні та взаємозалежності (розділ 1). Використання *функціонального методу* зумовлено формулюванням особливостей проведення окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій, а також інших процесуальних дій (підрозділи 3.1–3.3). *Статистичний метод* та *соціологічний метод* застосовувалися для аналізу оперативної та слідчо-судової практики, результатів здійсненого анкетування та узагальнення статистичних відомостей за темою дослідження (підрозділи 1.2, 1.3, 1.4, розділи 2 і 3). Застосування *документального методу* зумовлене пошуком прогалин в організаційно-тактичному забезпеченні проведення окремих слідчих (розшукових) дій та негласних слідчих (розшукових) дій (підрозділи 3.1–3.3). Застосовування *історико-правового методу* викликано потребою дослідження ґенези наукових поглядів щодо криміналістичної характеристики шахрайства у питаннях використання банківських

електронних платежів (підрозділ 1.1). *Метод синтезу* було використано у процесі формулювання висновків та пропозицій за темою дисертаційного дослідження.

Емпіричну основу дослідження становлять офіційні відомості статистичної звітності Генеральної прокуратури та результати узагальнення оперативної, слідчої та судової практики за 2011-2021 рр.; результати вивчення 156 кримінальних справ та 211 кримінальних проваджень за фактами вчинення шахрайства у сфері використання банківських електронних платежів (Вінницька, Волинська, Дніпропетровська, Донецька, Запорізька, Кіровоградська, Київська, Львівська, Луганська, Миколаївська, Одеська, Полтавська, Тернопільська, Харківська, Херсонська області та м. Київ); зведені результати опитувань 125 працівників прокуратури, 317 слідчих, 378 працівників оперативних підрозділів та 62 працівників експертних установ МВС України.

Наукова новизна отриманих результатів визначається тим, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням методики розслідування шахрайства у сфері використання банківських електронних платежів, у якій сформульовано ряд наукових домінант і рекомендацій, котрі відзначаються науковою новизною та мають вагоме теоретичне і практичне значення.

Основні наукові положення, що виносяться на захист:

уперше:

– надано інформативне наповнення криміналістичної характеристики визначених протиправних діянь, у якій послідовно охарактеризовано такі її елементи: спосіб учинення шахрайства, обстановку вчинення кримінального правопорушення, слідову картину, особу шахрая та особу потерпілого;

– доведено, що обстановку вчинення шахрайства у сфері використання банківських електронних платежів слід розглядати у фізичному сенсі, із урахуванням місця знаходження комп’ютерно-технічного устаткування, з якого здійснювалися шахрайські дії, а також у віртуально-просторовому, у

якому передається, зчитується та змінюється електронно-цифрова інформація, завдяки чому здійснюється втручання в облікові записи користувачів мережі Інтернет та знімаються грошові суми внаслідок незаконних транзакцій;

– виокремлено віктимогенні групи потерпілих, а саме: 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;

– сформовано напрямки тактичного забезпечення діяльності уповноважених осіб щодо реалізації комплексів слідчих (розшукових) дій та негласних слідчих (розшукових) дій для виконання окремих завдань кримінального провадження за фактами вчинення шахрайства у питаннях використання банківських електронних платежів;

удосконалено:

– криміналістичне наповнення типових способів вчинення шахрайства у сфері використання банківських електронних платежів під час користування онлайн-банкінгом, мобільним зв’язком, послугами в Інтернет-магазинах, зокрема, фішинг, сніфферінг, вішинг, кардінг;

– сукупність відомостей щодо слідів із матеріальних та особистісних джерел походження, із визначенням домінуючої ролі віртуальних (електронно-цифрових) слідів, що містяться: у пам’яті електронно-обчислювальних пристроїв, мобільному телефоні, електронному журналі банкомату (терміналу), на сервері інтернет-провайдера тощо, що у своїй сукупності формують слідову картину правопорушення;

– систему обставин, що підлягають встановленню у процесі розслідування шахрайства у сфері використання банківських електронних платежів, серед яких найважливішим є такі: обставини, котрі характеризують

вчинення шахрайства у питаннях використання банківських електронних платежів (відомості про час, місце вчинення шахрайства, відомості стосовно способу його вчинення, наприклад: використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, що викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, із персональних комп'ютерів користувачів; відомості щодо слідів протиправного діяння); визначення місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); засоби, що використовуються при скоєнні правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації; обставини, котрі відносяться до характеристики особи злочинця та особи потерпілого (кількість правопорушників – факт розподілу функцій серед шахраїв, завдання кожного з них);

– сукупність типових слідчих ситуацій початкового етапу розслідування досліджуваного виду шахрайства, у якій виділено такі: 1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай відомий – 19 %; 2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %; 3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %; 4) вчинено шахрайство у площині використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %;

– категорії свідків під час розслідування досліджуваної категорії протиправних діянь, а саме: особи, яким може бути відома інформація про обставини та умови протиправної діяльності, яку вони спостерігали; особи, які перебувають у родинному або іншому зв'язку із шахраєм; особи, яким відомі умови та обставини тих дій, у яких вони брали участь; особи, які певним чином сприяли вчиненню шахрайства, але самі про це не знали; особи, які були обізнані про обставини, що передували шахрайству; працівників банківських установ, яких було задіяно у використанні банківських електронних платежів.

– перелік питань, що слід з'ясовувати у підозрюваного, зокрема: за яких обставин вчинено шахрайські дії; які способи застосовувалися (використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів карток, що викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, із персональних комп'ютерів користувачів); які місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); які засоби використовувалися у процесі скоєння правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, а саме – VPN, браузери, графічні редактори, програми кодування інформації); яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчинення протиправних дій; який був порядок розподілу грошових коштів у членів ОГ чи ЗО; протягом якого періоду вчинялись протиправні діяння; які супутні кримінальні правопорушення було вчинено.

– перелік місць, де може проводитись обшук, зокрема: зберігання і обробки інформації про банківські електроні платежі, що зазнала злочинного впливу (67 %); знаходження комп'ютерного обладнання, що

використовувалося у процесі здійснення протиправного діяння (43 %); збереження інформації, отриманої злочинним шляхом (41 %); настання шкідливих наслідків (10 %);

дістало подальшого розвитку:

– окремі аспекти сутності та системи криміналістичної характеристики правопорушень, а також її значення у процесі їх розслідування, зокрема при формулюванні версій, взаємозв'язку між окремими науковими категоріями;

– деякі криміналістично вагомі ознаки особи злочинця, що їх було систематизовано та зведено в імовірний портрет відповідних категорій осіб;

– домінанти стосовно аналізу та оцінки первинної інформації, а також прийняття обґрунтованого рішення щодо відкриття кримінального провадження за фактом вчинення досліджуваної категорії протиправних діянь;

– організаційно-тактичні основи забезпечення проведення окремих слідчих (розшукових) дій для вилучення інформації з матеріальних та особистісних джерел із урахуванням завдань, що потребують вирішення під час їх підготовки та проведення;

– організація і тактика проведення окремих негласних слідчих (розшукових) дій, зокрема таких як спостереження за об'єктом, огляд кореспонденції, прослуховування телефонних переговорів, зняття інформації з транспортних та електронних систем;

– тактичне забезпечення підготовки та призначення основних видів експертиз у процесі розслідування шахрайства у сфері використання банківських електронних платежів.

Практичне значення одержаних результатів полягає у тому, що розроблені у дисертації положення та рекомендації можуть бути використані та використовуються у:

– *науковій діяльності* – для подальшого поліпшення окремих аспектів методики розслідування кримінальних правопорушень на базі сформульованих та означених теоретичних положень, висновків та рекомендацій (акт впровадження Дніпропетровського державного університету внутрішніх справ

від 20.11.2021 р.);

– *освітньому процесі* – під час викладання навчальних дисциплін «Криміналістика», «Кримінальний процес», «Криміналістичні засоби та методи розслідування кримінальних правопорушень», «Організація розслідування кримінальних правопорушень», «Оперативно-розшукова діяльність», а також під час підготовки підручників, посібників, текстів лекцій і навчально-методичних матеріалів, проведенні семінарів і практичних занять із кримінального процесу, криміналістики та оперативно-розшукової діяльності (акти впровадження Дніпропетровського державного університету внутрішніх справ від 11.11.2021 р.);

– *практичній діяльності* – для вдосконалення діяльності правоохоронних органів під час розслідування кримінальних правопорушень проти власності (акти впровадження Дніпропетровського НДЕКЦ МВС від 14.04.2020 р., Управління стратегічних розслідувань у Дніпропетровській області ДСР Національної поліції України від 11.05.2021 р.).

Апробація матеріалів дисертації. Основні теоретичні положення та висновки дисертації загалом, а також окремі її аспекти оприлюднені на науково-практичних конференціях та семінарах, зокрема на: «Актуальні проблеми забезпечення публічного порядку та безпеки в сучасних умовах: вітчизняний та міжнародний досвід» (м. Дніпро, 2019 р.), «Процесуальне та техніко-криміналістичне забезпечення досудового розслідування» (м. Харків, 2019 р.), «Правове життя сучасної України» (м. Одеса, 2020 р.), «Актуальні проблеми експертного забезпечення досудового розслідування» (м. Дніпро, 2020 р.), «Актуальні проблеми криміналістики та судової експертизи» (м. Дніпро, 2021 р).

Структура та обсяг дисертації. Робота складається із основної частини (вступ, три розділи, що логічно об’єднані у дев’ять підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 234 сторінки, із яких основний текст – 160 сторінок. Список використаних джерел складається із 219 найменування та становить 25 сторінок. Додатки викладено на 27 сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

1.1. Ґенеза наукових поглядів щодо криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів

Криміналістична характеристика – відносно нова категорія в криміналістиці загалом та в методиці розслідування кримінальних правопорушень зокрема. Водночас, вона має дуже важливе значення у процесі безпосереднього розслідування. Так, завдяки виокремленню в ній складових з’являється можливість для побудови криміналістичних версій на різних етапах кримінального провадження. Зокрема, наповнення окремих елементів надає відповідні переваги уповноваженій особі (слідчому, дізнавачу, прокурору) під час проведення певних слідчих (розшукових) та негласних слідчих (розшукових) дій. Тому вважаємо за необхідне дослідити криміналістичну характеристику шахрайства у площині використання банківських електронних платежів.

Сучасні Технології XXI сторіччя пронизують практично всі сфери нашого життя. Тотальна діджиталізація суспільства сприяє активному розвитку сучасних видів шахрайства, і, зокрема, шахрайства у питаннях банківських електронних платежів, як в Україні, так і в усьому світі [69, с. 77]. Згідно відомостям департаменту кіберполіції Національної поліції України спостерігається зростання даного виду шахрайства. Якщо в 2018 р. в Україні було зафіксовано близько трьох тисяч кримінальних проваджень, то вже в 2019 р. ця кількість збільшилась удвічі [35]. Такий вид

шахрайства стає дуже розповсюдженим і несе за собою величезні збитки як для громадян , так і для держави в цілому.

Як зазначає Г. О. Матусовський, методика розслідування злочинів окремими науковцями розглядається через призму дуалізму. Науковець наголошує, що окремі вчені визначають її саме як процес розслідування злочинів, зокрема як специфічну діяльність уповноважених законом органів, здійснювану на основі застосування засобів криміналістичної техніки, прийомів криміналістичної тактики, а також криміналістичних методів розслідування окремих видів злочинів. З іншого боку, окремі науковці визначають методику як розділ науки криміналістики, що містить систему комплексних криміналістичних рекомендацій по виявленню, розслідуванню і профілактиці окремих видів злочинів [113, с. 120].

Наразі, Ю. П. Аленін формулює структуру методики як поєднання таких елементів: криміналістична характеристика (для загальної методики) і окремих видів злочинів (для частинних методик); обставини, що підлягають встановленню і доказу; особливості порушення кримінальної справи; типові слідчі ситуації, особливості побудови версій і планування розслідування в цих умовах; організація первісного і наступного етапу розслідування в умовах постійної протидії злочинців; організація і використання тактичних операцій при розслідуванні злочинів; тактика проведення слідчих дій і оперативно-розшукових заходів; використання спеціальних знань; особливості взаємодії оперативних і слідчих апаратів правоохоронних органів з представниками суспільних і державних структур (види і форми) у процесі виявлення і розслідування злочинів [5, с. 244-250]. Як бачимо, науковець виділяє в методиці різні складові, зокрема й криміналістичну характеристику.

Доречною вважаємо думку В. А. Журавля з приводу того, що криміналістична методика виникла в результаті інтеграції та диференціації наукових знань та об’єднує в собі передові досягнення криміналістичної техніки й тактики, відповідно, щодо оптимальної організації розслідування

злочинів і судового розгляду певних категорій справ [47, с. 9]. Водночас, неодмінною складовою визначеної наукової категорії ми вбачаємо такий елемент як криміналістична характеристика шахрайства у сфері використання банківських електронних платежів.

Одразу підкреслимо, що єдина позиція щодо визначення сутності та наповнення вказаної категорії серед вчених-криміналістів відсутня. Так, наприклад, А. В. Старушкевич визначає її як засновану на практиці правоохоронних органів та криміналістичних досліджень модель системи зведених відомостей про криміналістично значущі ознаки виду, групи чи конкретного злочину, яка має на меті оптимізацію процесу розслідування злочинів [183, с. 9].

Наразі, В. В. Тіщенко вказує на те, що загальний метод включає в себе всі теоретичні положення криміналістичної методики і спрямовує їх на оптимальне формування окремих методик та подальшу адаптацію до розслідування у конкретному кримінальному провадженні. Він не може замінити всі теоретичні положення криміналістичної методики. Також автор зазначає, що метод, зокрема, слід розглядати як інструмент, спосіб, із допомогою якого утворюється окрема методика розслідування, але не фактор, який обумовлює зміст і структуру такої методики. Тобто оптимізація окремих методик розслідування залежить від правильного визначення принципів їх формування у теорії та застосування у практиці [191, с. 115-124].

Відтак, поділяємо думку групи науковців (А. В Іщенко, В. В. Тіщенко), які під міжвидовою (комплексною) методикою розуміють не просто сукупність окремих видових методик, а їх загальну інтегровану модель, що виконує системоутворюючу і методологічну функцію. Тобто розробки теоретичних основ криміналістичної методики ведуться в різних напрямках, що створюють нові підходи, уточнюючи, доповнюючи й оновлюючи відомі і, здавалося б, усталені наукові поняття та положення. Деякі дослідники наголошують, що не завжди відрізняються принципи науково-теоретичної

розробки приватних методик розслідування, з одного боку, і принципи застосування і побудови методики розслідування злочинів у практичній діяльності – з іншого. Наразі, інші науковці підкреслюють, що формування криміналістичної методики розслідування обумовлюється визначенням тих теоретичних і методологічних передумов, на основі яких можна виявити загальні закономірності та взаємозв'язки, властиві основним об'єктам криміналістичного наукового дослідження: діяльності з розслідування злочинів, з одного боку, та діяльності з їх вчиненню – з іншого. Автори наголошують на тому, що зазначеної мети можна досягнути за допомогою дієвого, системного та функціонального підходів, що утворюють у своїй системі загальний комплексний підхід, і будучи засобом пояснення, конструювання та прогнозування науково-методичних розробок[56, с. 180; 190, с. 7-9]. Отже, доходимо висновку, що дане дослідження є аналізом особливостей внутрішньовидової методики – методики розслідування шахрайства у сфері використання банківських електронних платежів.

Повертаючись до питання визначення криміналістичної характеристики, одразу звернемось до думки групи науковців (О. Н. Колесніченка, В. О. Коновалової), які наголошували, що до досліджуваної категорії належать відомості про криміналістично значущі ознаки злочинів певного виду. Зокрема, автори зазначають, що це система відомостей, яка спирається на структуру складу злочину (кримінальне право) та відповідну структуру предмету доказування (кримінально-процесуальне право). Також зазначені правознавці наголошують, що це система відомостей, яка включає дані про закономірні зв'язки статистичного характеру між ознаками злочинів певного виду. Підводячи підсумок, О. Н. Колесніченко та В. О. Коновалова сформулювали визначення поняття криміналістичної характеристики як системи відомостей (інформації) щодо криміналістично значущих ознак злочинів певного виду, що відбиває

закономірні зв’язки між ними і слугує побудові і перевірці слідчих версій в розслідуванні конкретних злочинів [79, с. 16-20].

Відтак, М. М. Єфімов акцентує увагу на тому, що «…криміналістична характеристика злочинів – це система відомостей про криміналістично значущі ознаки кримінально караного діяння, яка відображає закономірні зв’язки між ними і слугує побудові та перевірці слідчих версій для вирішення основних завдань розслідування» [45, с. 14-15]. Наразі, окрема група науковців (О. В. Батюк, Р. І. Благута, О. М. Гумін) сформулювали її як це систему відомостей про криміналістично значущі ознаки злочинів цього виду. Автори наголосили, що вона відображає закономірні зв’язки між цими ознаками і сприяє побудові та перевірці слідчих версій, що висуваються в процесі розслідування злочинів. Дослідники вказали, що 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 [115, с. 10]. Підтримуючи вказані позиції, дійсно зазначимо про те, що вважаємо криміналістичну характеристику інформаційною моделлю групи протиправних діянь певної категорії.

Зокрема, як показали результати опитування працівників правоохоронних органів [Додаток Б], 89 % респондентів вказали одним із найбільш перспективних напрямів підвищення ефективності розслідування побудову системи сталих кореляційних зв’язків між елементами криміналістичної характеристики шахрайства в сфері банківських електронних платежів.

А вже О. М. Селезньова дотримується думки, 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 [174, с. 212]. Тому ми поділяємо позицію

Р. Л. Степанюка, який наголошує, що кореляційні зв’язки між елементами криміналістичної характеристики певної групи злочинів і можливість їх встановлення та використання під час/у процесі вирішення завдань щодо виявлення і розслідування злочинів має найбільше значення при дослідженні окремих кримінальних правопорушень [185, с. 399]. Тобто автор підкреслює наявність сталих кореляційних зв’язків між елементами досліджуваної наукової категорії.

Підсумовуючи вищезазначене, сформулюємо поняття криміналістичної характеристики як інформаційної моделі групи протиправних діянь певної категорії, що має виражені складові зі сталими кореляційними зв’язками, що можуть використовуватись на будь-якому етапі розслідування.

Переходячи до питання наповнення елементами криміналістичної характеристики шахрайства у сфері банківських електронних платежів, одразу наведемо позицію вчених-криміналістів В. С. Кузьмічова, Г. І. Прокопенка, які вказують на наявність серед її елементів таких: предмет безпосереднього злочинного посягання (найрізноманітніші об’єкти органічного та неорганічного походження); спосіб вчинення злочинів в його широкому розумінні (обставини приготування, вчинення і приховування злочину, образ дії суб’єкта, що використовується для досягнення поставленої мети); типову «слідову картину» злочину в її широкій інтерпретації (сукупність джерел матеріальних та ідеальних відображень у навколишній матеріальній обстановці вчиненого злочину); особу злочинця (опис людини як соціально-біологічної системи, властивості та ознаки якої відображуються у матеріальному середовищі); особу потерпілого (для окремих видів чи груп злочинів: демографічні дані, відомості про спосіб життя, риси характеру, звички, зв’язки і стосунки, ознаки віктимності тощо) [103, с. 253].

Загалом, Ю. Я. Хамига надає власне визначення поняття «фінансове шахрайство» як «сукупності економічних відносин, що реалізуються юридичними або фізичними особами (переважно, без насильницьких дій) у процесі формування, розподілу і використання фінансових ресурсів (доходів)

шляхом обману або зловживання довірою чи службовим становищем із метою отримання економічної та/або іншої вигоди (особистої, корпоративної чи на користь третіх осіб), у 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].

Зокрема, зазначимо, що збут товарів і послуг між суб'єктами у мережі Інтернет відбувається через низку платформ. Характеристику дії таких платформ у своєму дослідженні надає група авторів (С. М. Ілляшенко, Т. Є. Іванова), зазначаючи, 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 віртуальну дошку оголошень зазвичай поділено 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 [54, с. 115].

А вже А. Ф. Волобуєв зазначає, що, зокрема, криміналістична характеристика розкрадань майна повинна відбивати традиційні елементи їх механізму але з урахуванням тієї специфіки, що накладає на них підприємницька діяльність, а також взаємні зв'язки з іншими злочинами, оскільки вони утворюють єдину технологію злочинної діяльності: особливості предмета посягання (матеріальні цінності, грошові кошти, цінні папери); обстановка вчинення злочину (загальноекономічні і правові умови підприємницької діяльності, організаційно-правові форми підприємств, стан контролю з боку відповідних державних органів, місце знаходження суб'єктів підприємництва та існування між ними певних відносин тощо); способи підготовки, вчинення і приховування розкрадання (прийоми створення сприятливих умов із метою заволодіння майном, прийоми безпосереднього заволодіння майном та його використання, заходи щодо

маскування розкрадання, вчинення супутніх розкраданню злочинів); сліди розкрадання (документів та речових доказів, свідчень осіб, що вказують на протиправне заволодіння майном); особливості суб'єкта розкрадання та супутніх злочинів (підприємця-фізичної особи, посадових осіб і службовців юридичної особи – суб'єкта підприємництва); особливості потерпілого від розкрадання (підприємця, окремих громадян) [26, с. 35].

Із цього приводу М. М. Єфімов акцентує, що криміналістична характеристика злочинів є категорією динамічною. Іншими словами, вона може змінюватись залежно від конкретних умов дійсності. Проте її використання може мати різні напрямки у діяльності працівників правоохоронних органів. Наприклад, за ознаками способу, місця та часу його вчинення може бути висунута версія щодо особи злочинця і, навпаки, при затриманні правопорушника та наявності даних про обставини злочину може бути побудована версія про вчинення цією особою інших, ще нерозкритих злочинів [44, с. 270].

Зі свого боку, С. В. Самойлов у своєму дисертаційному дослідженні, розглянувши криміналістичну характеристику шахрайств, що вчиняються з використанням мережі Інтернет, докладно розкрив зміст основних її елементів, окремо висвітлив класифікацію способів учинення, а також розробив теоретичні основи та практичні рекомендації щодо досудового розслідування зазначеної категорії кримінальних правопорушень [169]. У контексті зазначеного вважаємо за потрібне привести думку С. В. Чучко, який вказує на те, що дотепер залишається ряд невирішених питань щодо конкретних прийомів і операцій, спрямованих на підготовку, безпосереднє вчинення та приховування шахрайств, пов'язаних із придбанням товарів через мережу Інтернет [216, с. 235]. Тому дійсно вбачаємо потребу у виокремленні вказаного елементу криміналістичної характеристики визначеного протиправного діяння.

Як доречно наголошує Т. В. Коршикова, наразі є об'єктивна потреба в узагальненні та впорядкуванні наявних методичних рекомендацій щодо

розслідування шахрайств, учинених з використанням ЕОТ, із 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 цілісну методику. До допоміжних компонентів цієї концепції відносимо положення криміналістичної [86, с. 41].

Для вилучення віртуальних слідів з електронних носіїв обов’язковою має бути участь відповідних експертів, наявність спеціального програмного забезпечення, обчислювальної техніки та використанням розроблених наукових рекомендацій щодо їх застосування.

На основі дослідження матеріалів кримінальних проваджень та аналізу проведеного анкетування працівників правоохоронних органів, серед елементів криміналістичної характеристики шахрайства в сфері банківських електронних платежів, нами виокремлено наступні:

– спосіб учинення шахрайства;

– обстановку вчинення кримінального правопорушення;

– слідову картину;

– особу шахрая;

– особу потерпілого.

Підсумовуючи вищенаведене, зазначимо, що виокремлені складові елементи є взаємопов’язаними та характеризуються чіткою розшуковою спрямованістю, яка, наразі, забезпечує їх найоптимальніше використання у процесі доказування. Відтак, дослідження криміналістичної характеристики шахрайства в сфері банківських електронних платежів, потрібно для більш якісного та швидкого проведення розслідування. Загалом, визначена наукова категорія формулюється нами як інформаційна модель групи протиправних діянь певної категорії, яка має виражені складові зі сталими кореляційними зв’язками, що можуть використовуватись на будь-якому етапі розслідування. Слід зазначити, 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 такі елементи: спосіб учинення шахрайства, обстановку вчинення кримінального правопорушення, слідову картину, особу шахрая та особу потерпілого.

1.2. Криміналістичний аналіз способів вчинення шахрайства у сфері використання банківських електронних платежів

Шахрайство у сфері банківських електронних платежів, станом на кінець 2021 року, є однією з головних проблем не тільки України, а і всього світу. За допомогою такого виду шахрайства кожного року викрадаються з банківських рахунків десятки мільярдів доларів США у їх власників, та, на жаль, кількість постраждалих кожного дня тільки збільшується. Це стало можливим у зв'язку з розвитком всесвітньої мережі Інтернет та розвитком банківського сектору. На жаль, правоохоронна система відстає у своєму розвитку, у порівнянні з розвитком ІТ-технологій, що не скажеш про правопорушників, які займаються даним видом злочину**.** Такий вид кримінального правопорушення кваліфікується за ч. 3 ст. 190 КК України**,** яке вчиняється за допомогою електронно-обчислюваної техніки [96]. Це може бути ноутбук, персональний комп'ютер, планшет, смартфон з обов'язковим підключенням до всесвітньої мережі Інтернет. Тому з метою розгляду способів вчинення шахрайства в сфері банківських електронних платежів, розглянемо думки вчених, способи вчинення такого виду шахрайства, та визначимо їх криміналістичну характеристику [70, с. 137].

Ю. Я. Хамига акцентував увагу на тому, що «…специфіка функціонування фінансового ринку (зокрема, значна концентрація готівкових і безготівкових коштів, блискавичність проведення фінансових транзакцій,

розмаїття фінансових послуг та інструментів із різним рівнем захищеності й ліквідності, стрімке поширення інтернет-технологій та зростання клієнтської бази, великі масштаби здійснення міжнародних угод та їх висока адаптивність) формують сприятливе підґрунтя для реалізації різного роду шахрайських схем на фінансовому ринку» [199, с. 78]. Зі свого боку, В. О. Фінагеєв наголошує на тому, що «незаконний доступ до банківських рахунків технологічно поєднує пов'язані між собою кримінально карані діяння проти власності (ст. ст. 185, 190, 191 Кримінального кодексу (КК) України), у сфері господарської діяльності (ст. ст. 200, 205, 209, 231 КК України), використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. ст. 361, 361–1, 362 КК України), службової діяльності» [197]. Вищезазначеними науковцями проаналізовано цю проблему співвідносно з тематикою їх досліджень, а ми розглянемо, в свою чергу, способи шахрайства у сфері банківських електронних платежів.

Також зазначимо, що, як зазначають окремі автори, у період пандемії значно зріс обсяг онлайн-платежів в усіх сферах споживчого попиту крім туризму. Споживачі стали активніше використовувати методи безконтактної і безготівкової оплати. Учасників ринку це змусило більш уважно вивчити платіжні інструменти і почати підключати нові. Епідемія і суворі обмеження за короткий період привели до значних змін на споживчому ринку, спровокувавши зростання довіри споживачів до безготівкової оплати і масовий перехід у електронну комерцію, зростання числа мерчантів (торговців), транзакцій і, при цьому, кратне зростання числа шахраїв і «сірих схем» [37].

Наразі деякі вчені-криміналісти акцентують увагу на тому, що об'єктивну сторону злочину фактично можна ототожнити зі способом учинення злочину. Окрім того, автори відносять до способу віднесено й дії, що лежать за межами складу, тобто спрямовані на приховування самого злочину. Науковці наголошують, що специфіка способу вчинення злочину може вказувати на професійні навички вбивці, мотиви скоєння злочинного

діяння, соціальний і психологічний портрет злочинця. Підсумовуючи, зазначені вчені наголошують, що спосіб учинення злочину орієнтує слідчого на комплекс слідів, речових доказів, важливих для розслідування, і також він може сприяти встановленню особи потерпілого (мається на увазі характер попередніх відносин потерпілого і злочинця) [94, с. 181]. Підтримуючи зазначену позицію, наголосимо, що ми вважаємо спосіб вчинення кримінального правопорушення як кримінально-правовою, так і криміналістичною категорією.

Зі свого боку, С. М. Зав'ялов зазначає, що спосіб вчинення злочину як тріаду способів готування, вчинення та приховання злочину. Як відмічає науковець, ними виступає різновид діяльності людини, якій притаманні соціально-психологічні якості, орієнтувальні, сенсомоторні особливості суб'єкта [49, с. 5]. А вже К. Д. Заяць акцентував увагу на тому, що основні проблеми у слідчих виникають на стадії прийняття рішення про відкриття кримінального провадження, коли необхідно встановити ознаки складу кримінального правопорушення у фактичному акті добровільної передачі потерпілим майна або права на нього. Автор зазначав, що труднощі пов'язані з тим, що слідчому необхідно прийняти ключове процесуальне рішення на підставі аналізу дуже обмеженої інформації про подію. Окрім того, навіть у рамках відкритого кримінального провадження дуже складно сформувати систему доказів наявності злочинного наміру в діях шахрая [52, с. 207].

Зазначимо, що в методиці розслідування ще О. Н. Колесніченко виділяв спосіб підготовки до вчинення злочину, спосіб самого вчинення злочину і спосіб його приховування. Адже, як вказував автор, ці дії можуть бути скоєні в різний час, різними особами й мати різне кримінально-правове значення [80, с. 9-11].

А вже В. Н. Кудрявцев характеризував спосіб вчинення в кримінально-правовому розумінні таким чином: відповідний порядок, послідовність рухів і прийомів, застосовуваних особою, що утворюють дії з підготовки до злочину (підшукання, пристосування засобів, знарядь, створення умов тощо),

його вчиненню (дії, безпосередньо пов’язані із зазіханням на об’єкт), а також ті дії по приховуванню, що відбуваються до моменту закінчення злочину [101, с. 60-69]. Як бачимо, науковець виокремив ряд елементів, які входять до визначеної складової криміналістичної характеристики.

Наразі, В. П. Бахін наголошував на тому, що для виявлення злочинців і розкриття злочинів найбільш важливим є повноструктурний зміст способу. Автор вказану думку аргументував наступним чином: велику кількість суспільно-небезпечних діянь вчинює організована і професійна злочинність, для яких підготовка до здійснення злочинів є елементом їхньої життєдіяльності, а приховування злочинної діяльності представляє систему забезпечення цієї життєдіяльності [11, с. 199]. В розрізі вказаного, підтримуємо позицію Н. В. Павлової, яка головним і єднальним елементом, за допомогою якого можна дослідити виявлені у процесі аналізу зв’язки між всіма структурними елементами криміналістичної характеристики злочину, є спосіб учинення злочину [139, с. 20].

Розширюючи наведені визначення, І. Ш. Жорданія вказав, що спосіб безпосереднього вчинення злочину – це не просто сукупність певних актів поведінки, а їх визначена цілісна структура поведінки. В зв’язку з цим, вказана категорія, на думку автора, утворюється із взаємопов’язаних елементів, актів поведінки, спрямованих на підготовку, вчинення і приховування злочину. Ці акти поведінки – дії, операції, прийоми – сполучаються за певною ієрархією і субординацією як частини цілеспрямованої вольової діяльності [46, с. 73].

Зі свого боку, В. В. Тищенко до змісту способів вчинення злочину зараховує 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 [188, с. 18]. Ми згодні з наведеним визначенням і будемо розглядати спосіб вчинення

шахрайства визначеної категорії в цьому розрізі. З огляду на вивчення матеріалів кримінальних проваджень, дійшли висновку, що спосіб вчинення має місце у 100 % випадків [Додаток А].

Першою складовою способу є підготовка. Наприклад, О. В. Баланюк щодо підготовчих дій виділяв наступні їх групи: «…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)» [10, с. 195-196].

А вже С. В. Чучко вказував на існування таких способів підготовки до шахрайства: «…визначення найменування товару, що пропонуватиметься для продажу, створення його характеристик та отримання презентабельних фотографій; реєстрація та створення облікового запису особи в інформаційній телекомунікаційній системі під вигаданими анкетними даними; розміщення даних про товар; створення рівня довіри у покупців шляхом здійснення успішних цивільно-правових дистанційних угод та заповнення шкали позитивних оцінок; створення «окремої» електронної

адреси для здійснення переписки із потенційним споживачем; придбання «окремого» телефонного номеру для здійснення переговорів із потенційним споживачем; обрання способу здійснення розрахунків; реєстрація «електронних гаманців» у відповідних сервісах або отримання платіжної картки для перерахування грошей тощо» [210, с. 57].

На основі аналізу опитування працівників правоохоронних органів [Додаток Б], нами було встановлено, що мали місце такі підготовчі заходи до вчинення шахрайства у сфері банківських електронних платежів:

– підготовка відповідної електронно-обчислювальної техніки (комп'ютер, ноутбук, планшет тощо);

– створення програмного забезпечення для вчинення окремих видів шахрайства;

– вибір об'єкта, що буде предметом шахрайських дій;

– вибір кола осіб, які стануть жертвами шахрайських дій.

Наприклад, як повідомляє Департамент кіберполіції Національної поліції України, «Зловмисники, використовуючи шкідливе програмне забезпечення, отримали віддалений доступ до комп'ютера державного нотаріуса. Далі внесли зміни до реєстру прав власності на нерухомість в інтересах третьої особи. Причетним загрожує до восьми років за ґратами. Працівники кіберполіції Київщини спільно зі слідчими Васильківського відділу поліції встановили факт незаконного заволодіння нерухомістю у Києві завдяки використанню шкідливого програмного забезпечення. За попередніми даними, зловмисники надіслали електронного листа, що містив «вірус» державному нотаріусу. Таким чином вони отримали віддалений доступ до його комп'ютера. Далі правопорушники внесли неправдиві відомості до Державного реєстру речових прав на нерухоме майно. Відтак змінили право власності на нежитлову будівлю у центрі Києва площею близько 250 квадратних метрів. Співробітники кіберполіції встановили «замовника» таких послуг. У його оселі провели обшук із залученням спецпризначенців Київщини. За результатами вилучено комп'ютерну

техніку, що містить докази причетності до несанкціонованого втручання у роботу комп'ютера державного нотаріуса. Речові докази направлено на проведення відповідних експертних досліджень. Відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України» [193]. Як бачимо, в даному випадку було застосовано декілька способів підготовки до вчинення протиправних дій.

Стосовно безпосередньо способу вчинення шахрайських дій у сфері використання банківських електронних платежів зазначимо наступне. Окремі науковці наголошують на тому, що традиційною є класифікація способів за видом дій з використанням технологій, зокрема: «…1) технології зберігання і обробки інформації – на якому машинному носії та де зберігати, як зберігати (один або декілька файлів, архівом чи потрібна резервна копія тощо), як обробляти – які дії слід виконати з інформацією в процесі її обробки); 2) телекомунікаційні технології – як передавати дані комп'ютерними мережами; 3) технології мультимедіа та віртуальна реальність – як обробляти звукові та відеодані, як організувати віртуальну реальність для дистанційних ігор, аукціонів тощо; 4) технології програмування – як створювати програми для розв'язання реальних задач; 5) технології обробки зображень – як обробляти різні графічні дані; 6) технології розпізнавання (наприклад мови, відбитка пальця руки); 7) технології криптографії – як кодувати інформацію за допомогою шифрування» [178, с. 27].

А вже С. В. Самойлов запропонував «…класифікувати способи вчинення досліджуваних шахрайств за наступними підставами: а) шахрайства, що пов'язані з купівлею/продажем у мережі «Інтернет»; б) шахрайства, сутність яких полягає в отриманні коштів (майна) шляхом надсилання листів чи повідомлень; в) шахрайства, що для заволодіння коштами (майном) потребують розробки та розміщення в мережі «Інтернет» дублікатів або вузькоспеціалізованих сайтів для надання псевдопослуг; г) шахрайства, 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» [170, с. 176].

Отже, О. А. Самойленко на основі аналізу матеріалів слідчо-судової практики визначила типові на цей час в Україні способи вчинення кримінальних правопорушень у кіберпросторі, зокрема: «…1. Способи злочинних дій, пов'язані з функціонуванням соціально-орієнтованих мереж (від англ. social networks), діяльність яких заснована на так званій вікі (viki)-технології. 2. Способи злочинних дій, пов'язані з функціонуванням технології BitTorrent, створеної для передавання великих за обсягом файлів одним користувачем іншому або громадськості. 3. Способи злочинних дій, пов'язані з функціонуванням сервісів електронної дошки оголошень (від англ. абревіатури «BBC»). 4. Способи злочинних дій, пов'язані з функціонуванням технологій електронної комерції, створені для здійснення торгівлі через Інтернет. 5. Способи злочинних дій, пов'язані з функціонуванням технології електронної розсилки (e-mail, від англ. electronic mail); IP-телефонії (найчастіше через комп'ютерну програму Viber; програмне забезпечення із закритим кодом Skype), призначені для відправлення/отримання електронних повідомлень між користувачами комп'ютерної/телекомунікаційної мережі. 6. Способи злочинних дій, пов'язані з функціонуванням технологій електронних платіжних систем (англ. electronic payment systems), призначені для здійснення платіжних операцій через мережу Інтернет. 7. Способи злочинних дій, пов'язані з функціонуванням технології зберігання та обробки інформації. 8. Способи злочинних дій, пов'язані з функціонуванням шкідливого програмного забезпечення. (з англ. «crimeware», де «crime – злочинність, software – програмне забезпечення; часто як синонім застосовують «вірус»)» [163, с. 140-156].

Зі свого боку, О. В. Кришевич запропонував виокремити три основні групи способів шахрайств, учинених із використанням електронно-

обчислювальної техніки: «…1) способи незаконного доступу до банківських рахунків, пов’язані з використанням розрахунків платіжними дорученнями; 2) способи вчинення кримінальних правопорушень, пов’язаних із незаконним доступом до банківських рахунків, пов’язані з використанням операцій у сфері обігу банківських платіжних карток; 3) способи вчинення кримінальних правопорушень, пов’язані з використанням інших засобів доступу до банківських рахунків». Автор наголошує на тому, що йдеться, наприклад, про: внесення неправдивих відомостей до автоматизованої системи банківської установи; розміщення фіктивного повідомлення на електронній дошці оголошень або інтернет-аукціоні; несанкціоноване втручання в роботу бортового комп’ютера транспортного засобу з метою ввести в оману щодо показників [99].

Також доречною вважаємо думку С. В. Самойлова, який акцентував увагу на тому, що серед способів маніпуляції інформацією, як видом обману, при вчинені шахрайств із використанням мережі «Інтернет», необхідно виокремити наступні: а) умовчання; б) селекція; в) відволікання; г) перекручення; д) попереднє програмування дій. Досліджуючи такий спосіб, як «зловживання довірою», автор відмітив, що відсутність у самій нормі кримінального закону визначення такого поняття викликає неоднозначність його тлумачення у правозастосовній і науковій діяльності. За результатами вивчення слідчої та судової практики вчений довів, що шахрайству, учиненому з використанням мережі «Інтернет», притаманні одночасно й обман, і зловживання довірою [168, с. 4].

А вже С. В. Чучко стверджував, що «…шахрайські дії здійснюються різними особами. Утім, залежно від суб’єкта, способи вчинення шахрайства у мережі Інтернет можна поділити на ті, що: учинені від імені особи, яка діє як фізична особа-підприємець, що пропонувала товар; вчинені від імені юридичної особи, яка оформила відповідні документи для здійснення підприємницької діяльності, дані про яку розміщені в Єдиному державному реєстрі юридичних осіб; учинені від імені вигаданої особи, анкетні дані якої

не відповідають дійсності; вчинені особою, яка мала намір придбати товар (покупцем) [216, с. 236].

Наразі, дослідниця Т. В. Охрімчук акцентувала увагу на тому, що основним елементом криміналістичної характеристики шахрайства з фінансовими ресурсами є спосіб вчинення. Авторка зазначила, що вказаний елемент складається із системи взаємопов'язаних дій щодо підготовки, вчинення та приховування слідів злочину та полягає, перш за все, у введенні в оману, у наданні завідомо недостовірної інформації, зокрема, шляхом подання підроблених документів кредитору [137, с. 95].

Також зазначимо, що окрема група науковців вказувала на те, що обман може мати місце щодо предмета (його ціни, якості, кількості і т.п.), особи (її службового або громадського стану, професії) тощо. Автори зазначали, що зловживання довірою під час шахрайства є своєрідною формою обману, що полягає в недобросовісному використанні злочинцем певних відносин, що вже склалися між ним і потерпілим. Така форма обману може виникнути тоді, коли між потерпілим і винною особою вже існують стосунки, що і породжують певну, можливо лише зовнішню, довіру між ними. У зв'язку з цим потерпілий передає майно винній особі на підставі довіри до неї та помилкової впевненості у правильності її дій [194, с. 421]. Погоджуючись із цим твердженням, зазначимо, що такий спосіб шахрайства притаманний більшості з досліджених нами.

Основними способами вчинення шахрайства у сфері банківських електронних платежів в Україні можна виділити такі:

– фішинг;

– сніфферінг;

– вішинг;

– кардинг.

Фішинг – один з видів інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів, паролів, даних особових рахунків і банківських карт [116].

Переважно використовується метод проведення масових розсилок від імені популярних компаній або організацій, що містять посилання на помилкові сайти, зовні відрізнити від справжніх. Зовні здається, що фішингові повідомлення приходять від імені популярних організацій або компаній (як LiqPay, Skrill, UPS, урядові організації або банківські установи), однак насправді вони є підробленими [171, с. 103].

У листах зловмисники ввічливо попросять оновити або підтвердити вірність персональної інформації, нерідко згадують будь-які проблеми з даними. Пізніше користувача перенаправляють на підроблений сайт, що дуже важко відрізнити від справжнього, де користувача просять ввести облікові дані. Якщо зловмисники отримають необхідну інформацію, це може призвести до крадіжки персональних даних або коштів [158, с. 57].

Різновидами фішингу, як доречно наголошує Т. В. Коршикова, є: 1) фішингові сайти; 2) фішингові електронні листи; 3) фішингові SMS-повідомлення [87, с. 52].

Так, наприклад, під час досудового розслідування було встановлено, що невстановлені особи, які шахрайським шляхом, шляхом обману під приводом купівлі товару заволодівають коштами громадян через фішингові (підроблені) сайти Нової Пошти та OLX, у подальшому дані кошти перекидають на відповідні карткові рахунки, що обслуговуються наступними платіжними (банківськими) картками. Під час досудового розслідування виникла необхідність отримання відповідних документів, що слугували підставою для відкриття даних рахунків, зокрема копії паспортів, заяв та анкет. Оскільки наведені документи надають можливість органу досудового розслідування використовувати їх як докази у вказаному кримінальному провадженні, а також унеможливить їх зміну, або знищення у зв’язку із закінченням термінів зберігання вищезазначеної документації та інформації з інших причин. Тому судом було прийнято рішення задовольнити ухвалу [182].

Іншим прикладом буде така ситуація. Отже, за даними Департаменту кіберполіції Національної поліції України: «Фігуранти створили десяток фішингових інтернет-майданчиків оголошень, де користувачі вводили свої банківські дані. Таким чином зловмисники ошукали потерпілих на понад мільйон гривень. Злочинну схему викрили працівники управління протидії кіберзлочинам в Дніпропетровській області спільно зі слідчим відділом Дніпровського районного управління поліції. Троє 19-річних місцевих мешканців створили близько десяти фішингових сайтів, які повністю копіювали дизайн іноземних інтернет-майданчиків оголошень. Користувачі, громадяни країн Європи та Америки, на фейкових ресурсах вводили свої банківські дані для розрахунку. Надалі зібрані дані карток зловмисники «підв'язували до системи безконтактної оплати на телефонах. З рахунків потерпілих фігуранти сплачували покупки у магазинах побутової техніки. Наразі поліцейські встановлюють коло ошуканих. Попередня сума збитків сягає понад мільйон гривень. В оселях фігурантів правоохоронці провели обшуки та вилучили мобільні телефони, комп'ютерну техніку та банківські картки. Вилучене направлено на проведення експертних досліджень» [64].

Одразу приведемо рекомендації Кіберполіції щодо того, як громадянам убезпечити себе від фішингових ресурсів:

«– не переходити за підозрілими гіперпосиланнями, надісланими сторонніми;

– для онлайн-шопінгу використовувати лише перевірені ресурси;

– уважно перевіряти URL-адресу необхідного сайту, адже один зайвий символ може означати, що ви потрапили на фішинговий сайт;

– нікому не повідомляти дані карти, паролі та інші дані, що можуть використовуватися для підтвердження платежів;

– у разі купівлі на платформі оголошень, обговорювати деталі угоди лише в чаті цієї платформи і не переходити у месенджери» [64].

Говорячи про сніферінг, варто зазначити, що М. Ю. Комаров в своєму дослідженні акцентує увагу на тому, що даний спосіб дуже популярний для

захоплення та розбору мережевого трафіку [81]. Тобто завдяки сніферінгу шахрай може отримати відомості про топологію мережі, потоки, адреси в ній тощо.

Так, як повідомляв Департамент кіберполіції Національної поліції України, «Фінансова установа зазнала понад 1,5 мільйона гривень збитку через внесення неправдивих відомостей до її інформаційних систем. За це причетним загрожує до восьми років ув'язнення. Кіберполіція спільно зі слідчими Святошинського управління поліції Києва встановила факт підробки документів, необхідних для укладання кредитного договору та у подальшому незаконного отримання кредиту. Таким чином, банку було нанесено понад 1,5 мільйона гривень збитку. Наразі співробітники поліції перевіряють працівників банку на причетність до внесення неправдивих відомостей в інформаційні системи фінустанови. Правоохоронці встановили особу фігуранта – ним виявився житель столичної області. За місцем проживання чоловіка провели обшук та вилучили комп'ютерну техніку, яка містить докази причетності до вчинення вказаного правопорушення. Під час обшуку також були залучені бійці полку особливого призначення поліції Київщини. Наразі правоохоронці встановлюють можливих спільників фігуранта та остаточну суму збитків. За даним фактом відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України» [63]. Відомості про вказане були внесені за допомогою сніферінгу.

Вішинг (англ. Vishing – від voice phishing) – вид телефонного шахрайства, що дозволяє красти у клієнтів банків конфіденційну інформацію. Клієнт отримує дзвінок від автоінформатора, який повідомляє, що з картою, наприклад, виробляються шахрайські дії, і дає інструкції – передзвонити за певним номером. Далі, слідуючи інструкціям автовідповідача, клієнт повинен повідомити або ввести на клавіатурі телефону реквізити карти. Іноді зловмисники самі дзвонять жертвам, переконуючи, що є співробітниками банку. У банках стверджують, що в телефонних розмовах з клієнтом ніколи не запитують повний номер карти,

тим більше не вимагають повідомляти ПІН-код. Щоб прояснити ситуацію, необхідно передзвонити в банк за номерами телефонів, вказаними на офіційному сайті кредитної організації [187, с. 38].

Так, наприклад, у вересні 2020 р. в м. Мелітополі співробітники Служби безпеки України блокували діяльність колл-центру, учасники якої викрадали кошти з банківських рахунків Сбербанку. Слідство встановило, що злочинну схему організували троє жителів Мелітополя. У центрі міста вони обладнали незаконний колл-центр, де «працювало» 54 оператора. Вони видавали себе за співробітників банку, дзвонили клієнтам і отримували від них інформацію про CVV-коди, номери і пін-коди платіжних карт. Для «роботи» з клієнтами банків з Росії зловмисники використовували маршрутизацію міжнародного телефонного трафіку [70, с. 138].

Кардинґ (англ. Carding) – протиправна діяльність у сфері обігу платіжних карток та/або конфіденційної інформації про їх реквізити [43].

Найбільш загальні рекомендації по запобіганню вказаного виду шахрайства, виглядають наступним чином:

«– не передавати свою картку в чужі руки, стежити за тим, щоб картка використовувалася лише за призначенням (щоб неможливо було застосувати портативний скімінговий пристрій, захований під одягом, наприклад, офіціанта або працівника автозаправних станцій, продавця магазину тощо);

– проявляти пильність і уважність при користуванні банкоматом, звертати увагу на нестандартні елементи конструкції – накладну клавіатуру, що використовується для зчитування PIN-коду. У разі скімінгу така клавіатура розташовується, як правило, вище рівня корпусу банкомату, легко від неї відділяється і, найчастіше, під накладною можна побачити частину оригінальної;

– звертати увагу на встановлені мікро-відеокамери на самому банкоматі, які можуть бути змонтовані як в козирку банкомату, так і замасковані під супутні предмети банкомату, наприклад, рекламні матеріали;

– мінімізувати випадки використання банківської картки в місцях, що

викликають підозру. По можливості, використання банківської картки в приміщеннях, які добре проглядаються;

– зняття готівкових коштів та інші банківські операції, по можливості, проводити в одному і тому ж банкоматі, запам'ятавши його зовнішній вигляд;

– по можливості, набирати пін-код швидко, використовуючи кілька пальців руки відразу – так зловмисникам буде складніше розпізнати ваші рухи. По можливості, прикривати набирання пін-код іншою рукою, сумочкою або будь-якими іншим предметом;

– якщо банк-емітент банківської картки має в своєму сервісі послугу швидкого попередження власника картки про факти списання (наприклад, за допомогою СМС)

– інформацію про PIN-код, смс пароль, букв і цифр зі зворотного (не лицьового боку карти) не передавати знайомим і незнайомим людям;

– використовувати банківські картки з вбудованим мікрочипом» [59].

Залишилось розглянути останню складову способу вчинення, а саме – приховування. Стосовно вказаної категорії ще М. В. Салтевський наголошував, що він реалізується як самостійне явище лише тоді, коли злочин вчинений, у багатьох випадках зареєстрований і щодо нього ведеться розслідування. Автор акцентував увагу на тому, що усе це докорінно перебудовує систему його детермінуючих факторів. Вчений зазначив, що 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 [159, с. 426].

В свою чергу, П. В. Малишкін стосовно способу приховування кримінального правопорушення відмічав, що для перспективи приховування суспільно-небезпечного діяння злочинець найчастіше формує так звані «штучні» умови для ефективної реалізації задуманого. В результаті здійснення ним комплексу дій для приховування злочину в обстановці злочину відображаються основні властивості ознак вибраного їм способу

злочину. З інформації, отриманої з слідів, які особа лишила на місті події в ході здійснення дій з приховування злочину, стає можливим визначити спосіб їх вчинення, дії злочинця, вчинені з цією ціллю, розпізнати спосіб приховування [112, с. 22].

На основі аналізу опитування працівників правоохоронних органів [Додаток Б], 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 СРД, НСРД та інших процесуальних заходів;

– відмова від дачі показань.

Таким чином, існує безліч способів шахрайства у сфері банківських електронних платежів. Шахраї спритно і освідчено адаптуються до ходу прогресу, винаходячи нові шахрайські схеми. Власникам банківських карт, користувачам мережі Інтернет необхідно бути обізнаними про способи шахрайства. Крім того, проявляти грамотність і обережність при користуванні онлайн-банкінгом, мобільним зв’язком, послугами в Інтернет-магазинах, уважно заповнювати анкети і форми на різних сайтах [70, с. 139].

1.3. Обстановка та умови вчинення шахрайства в сфері банківських електронних платежів. Слідова картина

Кожне кримінальне правопорушення, у тому числі й шахрайство у сфері банківських електронних платежів, вчиняється у певних умовах та в обстановці, що характеризуються просторово-часовими характеристиками. Тому, існування у структурі криміналістичної характеристики обстановки вчинення злочину не викликає ніяких сумнівів.

Натомість, як показав проведений нами аналіз, з приводу змістової частини цього елемента криміналістичної характеристики виникає найбільше дискусій.

Зокрема, Н. В. Олиндер визначає обстановку вчинення злочину як систему певним чином взаємодіючих між собою в конкретних умовах місця і часу фактів об'єктивної реальності, що обумовлюють спрямованість і хід поведінки людей в подію злочину, а також детермінують характер, механізм і умови матеріального відображення процесів, що відбуваються і явищ у вигляді характерної, щодо стійкої сукупності слідів, дослідження яких дозволяє судити про сутність того, що сталося» [126, с. 13]. А вже В. А. Динту розкриває зміст поняття обстановки злочину як системи даних, що відображає матеріальні, мікросоціальні та морально-психологічні умови підготовки, вчинення та приховування злочину [36, с. 8].

Деякі вчені до поняття «обстановка вчинення злочину» відносять й психологічні складові, що містять в собі взаємини між потерпілим та злочинцем, їх поведінку [114, с. 37]. Утім, більшість вчених сходяться на тому, що немає таких матеріальних об'єктів, виникнення, розвиток і зникнення яких не проходило б у певному місці й в певний час [177, с. 12].

Проведений аналіз показує, що більшість вчених передбачають фізичну (матеріальну) складову у змісті обстановки вчинення злочину. Проте, на нашу думку, не слід розглядати обстановку вчинення злочину тільки в межах сукупності матеріальних (фізичних) умов, в яких діяв злочинець.

У контексті даної проблематики Г. А. Матусовський наголошує, що обстановка вчинення злочину охоплює більш широке коло явищ на певному об'єкті, де відбувається злочин, аніж матеріальні умови. До таких можна віднести: 1) нормативно-правове регулювання; 2) майно, що перебуває у власності (управлінні) та його види; 3) структуру і профіль роботи підприємства, його ділові, виробничі та інші зв'язки; 4) технологічний процес, характер, вид виконуваних операцій; 5) документообіг, облік, звітність, контроль, охорона; 6) склад, службове становище працівників, їх

професійні й особистісні якості, ділові та інші зв’язки між ними; 7) відношення працівників до цінностей і виробничих операцій; 8) діяльність працівників; 9) наявність різного роду недоліків у діяльності, контролі, обліку, охороні [113].

Може виходити за межі фізичної (матеріальної) складової й обстановка вчинення шахрайства в сфері банківських електронних платежів.

На цьому наголошує й А. І. Анапольська, на думку якої умови вчинення злочинів з використанням конфіденційних даних про реквізити справжніх платіжних карток включає в себе речові, технічні, соціально-психологічні, а також просторові чинники [7].

Користуючись поняттям умови, О. В. Курман хоча і має на увазі матеріальне середовище, але наразі науковець ураховує у її змісті технічну оснащеність, систему обліку, технологію проведення кредитних операцій, використання обчислювальної техніки, сучасних методів обліку, електронного зв’язку з кореспондентами банку тощо [107, с. 45].

Відтак, слід звернути увагу на думку Б. В. Черняховського, який зазначає, 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 [208, с. 59]. Завдяки електронним пристроям різного рівня складності, підключених до глобальної або локальної мережі, виникає віртуальне середовище [214, с. 39], і кожний користувач мережі Інтернет та його комп’ютер діють автономно та формують єдину транснаціональну мережу, що виходить за межі географічної концепції чітких кордонів [8, с. 27].

Натомість, слід наголосити, що сервери, з яких здійснюються банківські платежі, знімаються шахраями суми грошей з рахунків потерпілих, здійснюється втручання у облікові записи користувачів мережі Інтернет тощо, знаходяться у фізичному просторі і мають свою ір-адресу.

Отже, обстановку вчинення шахрайства в сфері використання банківських електронних платежів слід розглядати як у фізичному сенсі, із врахуванням місця знаходження комп'ютерно-технічного устаткування, з якого здійснювалися шахрайські дії, так і як віртуальний простір, в якому передавалася та зчитується цифрова інформація.

Як показало опитування практичних працівників, 67 % респондентів вважають, що обстановку та умови вчинення шахрайства певною мірою визначає вид платіжної системи, через які здійснюються електронні платежі [Додаток А].

Згідно Закону України «Про платіжні системи та переказ коштів в Україні», під платіжною системою розуміється платіжна організація, учасники платіжної системи та сукупність відносин, що виникають між ними при проведенні переказу коштів. При цьому, законодавець визначає проведення переказу коштів обов'язковою функцією, що має виконувати платіжна система [152].

У цьому розрізі К. В. Преловський, проводячи аналіз інфраструктури банківської системи України, наголошує, що в нашій державі на даний момент функціонує ряд платіжних систем, серед яких є 2 державні («Система електронних платежів», «Національна платіжна система «Український платіжний простір»), 12 внутрішньобанківських платіжних систем («Freesend», «Гроші блискавкою», «Металкарт», «Миттєвий переказ», «Фінекспрес», «За мить», «Eximcash», «Онікс», «Unite express», «Аваль-експрес», «Акордбанк-експрес», «Глобус»), 9 платіжних систем, платіжними організаціями яких є банки («Welsend», «Софт», «Privatmoney», «Flashpay», «The money», «Система термінових переказів», «Швидка копійка», «Telegraf», «Ibox money transfer», «Avers №1»), 15 платіжних систем, платіжними організаціями яких є небанківські установи («Поштовий переказ», «Інтерпейсервіс», «Фінансовий світ», «Розрахункова фондова система», «Глобалмані», «Tyme», «Webmoney.ua», «Укркарт», «Mosst payments», «Forpost», «Paypong», «Електрум», «Лео», «Платисервіс», «City

24»), 3 міжнародні карткові платіжні системи («American express», «Mastercard», «Visa») та 7 міжнародних систем переказу коштів («Moneygram», «Western union», «Meest», «Ria», «Хазри», «Intelexpress», «Sigue money transfer») [147, с. 96]. За матеріалами Н. О. Коваль та М. В. Борщ, функціонування платіжних систем в Україні взагалі має тенденцію до глобалізаційних процесів і все більше використовуються міжнародні платіжні системи різних типів, незважаючи на існування внутрішньодержавних. Це можна пояснити більшою надійністю, досвідом їх використання у провідних банківських системах світу [76].

Наразі, жодна платіжна система не може повністю запобігти вчиненню шахрайських дій. Так, прямими загрозами для діяльності електронних платіжних систем є кібератаки, направлені на таке:

1) викрадення приватних даних користувачів платіжної системи;

2) ураження платіжної системи з метою паралізації її роботи шляхом внесення змін у алгоритм роботи системи, зашифровки файлів тощо;

3) отримання безпосереднього доступу до банківських електронних рахунків з метою викрадення коштів власників;

4) пряме втручання у роботу системи з боку людини, направлене на отримання персональних даних користувачів платіжної системи, ураження її роботи тощо [147, с. 97].

Зі слів А. І. Анапольської, основними умовами, що сприяють вчиненню досліджуваного виду шахрайств є:

– відсутність практики постійної зміни паролів та кодів доступу до системи електронних розрахунків;

– відсутність між працівниками банку розмежування доступу до комп’ютерної інформації про електронні рахунки;

– надання комплекту комп’ютерної техніки у безконтрольне користування співробітникам;

– відсутність контролю за порядком проведення електронних розрахунків тощо [7].

Утім, пропонуємо до складу обстановки вчинення шахрайства у сфері використання банківських платежів віднести й систему інформаційних ресурсів, пов’язаних із функціонуванням платіжних систем, через які проводяться транзакції.

Досліджуючи обстановку функціонування платіжних систем у банківській сфері, низкою дослідників виявлено, що в умовах зменшення кількості клієнтів, що утримують або знімають кошти з банківських рахунків завдяки доступності цифрового банкінгу та безготівкових платежів, необхідність фізичної присутності клієнтів при наданні банківських послуг постійно зменшується. Наразі, із зменшенням кількості банківських філій та зростанням кількості користувачів цифрового банкінгу виникає необхідність у розширенні автоматизації банків з метою запобігання загрозам цифрового шахрайства, що постійно еволюціонують. Крім того, пришвидшення процесингу платежів може нести новий виклик, оскільки банки матимуть менше часу на аналіз операцій на предмет шахрайства. Пришвидшення платежів також несе в собі ризик зменшення розміру відшкодування збитків, понесених в результаті шахрайства, оскільки проходження офшорних платежів через велику кількість рахунків здійснюватиметься за лічені секунди. У пошуках збалансованості між заходами із запобігання ризику шахрайства та відносинами з клієнтами, банки застосовують засоби запобігання та виявлення шахрайства у режимі реального часу та встановлюють обмеження і додаткові засоби аутентифікації для операцій з високим ступенем ризику шахрайства, прагнучи зменшити його під час онлайн-платежів. Аутентифікація псевдонімів також є ключовим моментом, зокрема у випадку операцій із стягнення платежів у режимі онлайн (pull payments), коли шахраї можуть вимагати здійснити платіж, представившись як комунальне підприємство або підприємство зв’язку [9, с. 12].

Зазначене свідчить, що обстановку та умови вчинення шахрайства у сфері електронних банківських платежів визначає й рівень інформаційної безпеки у банківській сфері (на думку 87 % респондентів) [Додаток А]. Адже

банки, що є членами платіжних систем, не завжди приділяють достатньої уваги безпеці розрахунків та захисту інформації, а також не здійснюють належним чином моніторинг та відеоспостереження за банкоматами. Відтак, переважно картки міжнародних платіжних систем, що їх емітують українські банки, є недостатньо захищеними, адже носієм інформації даного платіжного інструменту є магнітна смуга, а не чип. Шахрайство з використанням реквізитів платіжних карток в Інтернеті характеризується збільшенням кількості фішингових сайтів, електронних листів та SMS-повідомлень, за допомогою яких зловмисники отримують реквізити платіжних карток у держателів платіжних карток, емітованих банками України. Наявність в Інтернеті багатьох різних електронних платіжних систем, пропонування великою кількістю банків послуг інтернет-банкінгу, доступність Інтернету та розповсюдження зловмисниками інформації щодо реквізитів платіжних карток перетворили фішинг у дуже поширений та прибутковий вид шахрайства. Всі ці фактори дають можливість, особливо для молодих громадян, отримувати «легкі гроші» фактично безкарно, тому такий вид шахрайства набуває все більшого розповсюдження у країнах СНД та Європи. Щодня встановлюються тисячі підроблених фішингових веб-сайтів в режимі онлайн, котрі, заманюючи будь-яку кількість споживачів, спричиняють проблеми та втрати ними коштів [200].

Певні вчені наголошують на віддаленості об’єкта злочинних посягань, що може перебувати за тисячі кілометрів від місця скоєння злочину [65, с. 347]. До того ж, серед шахраїв відбувається оперативний обмін інформацією щодо оперативного переведення електронних коштів у готівку тощо на території різних країн [211, с. 93]. Аналіз судово-слідчої практики засвідчив, що дії шахраїв можуть складатися із ряду операцій, пов’язаних із втручанням у облікові записи, електронні скриньки та інші електронні ресурси користувачів мережі Інтернет, які тривають у часі та здійснюються на необмеженій території [Додаток Б]. У зв’язку із чим набуває

актуальності встановлення часово-просторових характеристик вчинення шахрайських дій.

Проведений аналіз дозволяє зробити висновки, що більшість науковців здебільшого розглядають ознаки місця, часу та обстановки у взаємозв'язку між собою. Проте, є й протилежні думки. Зокрема, С. І. Селецький вважає, що місце і час не входять у зміст поняття «обстановка», проте, у поєднанні з останнім, утворюють ситуацію вчинення злочину. На його думку, компоненти ситуації доповнюють один одного, зумовлюють якісно новий зміст зовнішнього оточення злочинного діяння, збільшують або зменшують комплекс норм, що забороняють якість дії або вимагають певної поведінки [175, с. 59]. Т. В. Дубно також категорично не погоджується з тим, що місце і час необхідно включати у зміст поняття обстановки. Апелюючи «законами діалектики», вчений вважає, що «чистого» часу та простору, не пов'язаного з матеріальними об'єктами, не існує [38, с. 377].

Натомість, ми не можемо погодитися з позицією щодо утворення ситуації через компоненти місця та часу замість обстановки вчинення злочину. Не можемо й підтримати й тезу щодо неможливості існування часу та простору, не пов'язаного з матеріальними об'єктами.

У контексті даної проблематики звернемо увагу на той факт, що місце вчинення злочину у криміналістиці традиційно розуміється як ділянка місцевості або приміщення, будівля, в межах яких було вчинено злочин та виявлено сліди [92, с. 166]. Разом з тим, О. Л. Мусієнко наголошує на тому, що при розслідуванні шахрайства місце вчинення злочину та місце події не завжди становлять єдиний комплекс. Місце злочину одне – це місце вчинення шахрайства, а місць події, пов'язаних із цією подією, може бути декілька: місце виготовлення підроблених документів, місце транспортування вилучених матеріальних цінностей тощо [121].

Як вже було зазначено, під час вчинення шахрайства, пов'язаного із використанням комп'ютерних технологій, у тому числі в сфері банківських електронних платежів, більшість злочинних дій дійсно вчинені у

віртуальному просторі і розтягнуті у часі та просторі. Як свідчить аналіз судово-слідчої практики, шахраї, перед тим, як заволодіти грошима потерпілих, здійснюють низку підготовчих дій (100 %) [Додаток А, Б].

Зокрема, шахрайські дії можуть починатися з виявлення слабких місць у захисті, шляхом автоматичного перебирання абонентських номерів («угадування коду»), дії «хакерів», з'єднання з тим чи іншим комп'ютером, підключеним до телефонної мережі, використання чужого імені (пароля) за допомогою існуючої помилки в логіці побудови програми та ін. [122]. До того ж, шахраї можуть використовувати троянських коней для отримання паролів, зокрема вони можуть використовуватися у сфері банківських шахрайств, коли невеликі суми грошей знімаються з законних рахунків і передаються до секретних рахунків. За допомогою трояну можливо отримати доступ до чужого поштового ящику. Для цього проводиться розсилання електронних листів з вбудованими вірусами, вірус вбудовується не в сам лист, а лист лише містить посилання на вірус, зазвичай зміст листа має чимось «зачепити» користувача, він повинен бути таким, на який користувач не зможе не відреагувати. Прикладами троянів є: DarkComet RAT, SpyEye, Carberp та ін. [157, с. 106].

Місце вчинення безпосередніх протиправних дій і місце, де наступають наслідки злочину і де вони можуть бути виявлені, можуть перебувати на досить таки великій відстані одне від одного, наприклад, в різних приміщеннях однієї організації, в різних містах однієї країни і навіть в різних країнах чи й континентах [18, с. 9].

С. В. Шапочка, досліджуючи проблеми боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет, у тому числі при здійсненні банківських платежів, наголошує на тому, що анонімність та можливість використання шахраями систем зв'язку з вільним доступом, можливість придбання необмеженої кількості sim-card, створення акаунтів на різних ресурсах, сервери яких розташовані і належать різним країнам, суттєво ускладнює процес розслідування [211, с. 93]. Вказані та інші причини

ускладнюють встановлення просторово-часових параметрів у кримінальних провадженнях.

Хоча аналіз криміналістичної літератури показав, що не всі вчені погоджуються із складністю визначення часу. Зокрема, В. О. Голубєв стверджує, що встановлення часу вчинення кримінальних правопорушень з використанням ЕОТ не складає великих проблем, адже за допомогою програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволить за відповідною командою вивести на екран дисплею інформацію про день, години, хвилини та секунди виконання тієї або іншої операції [31, с. 101].

Зокрема, слід звернути увагу на думку М. В. Карчевського та Ю. О. Кучера, які пропонують розмежовувати юридичний та фактичний час вчинення злочину. Юридичний час вчинення злочину, на думку дослідників, це загальна нормативна інформація про темпоральний вимір юридичного діяння та причинно пов'язаних із ним передбачених кримінальним законом наслідків. Фактичний час вчинення злочину – конкретна фактична інформація про тривалість реального діяння та причинно пов'язаних із ним певних наслідків, що настали в межах відповідного темпорального виміру, передбаченого певною нормою Особливої частини КК [95, с. 315]. Так, Г. К. Авдєєва та С. В. Стороженко вважають, що час роботи користувача в мережі Інтернет на певній електронно-обчислювальній техніці можна встановити за спеціальним log-файлом (журналом), а додаткові відомості про вид, порядок і час підключень користувача до мережі і збіг цих даних з logфайлом провайдера може слугувати вагомим доказом використання саме цієї електронно-обчислювальної техніки для вчинення шахрайства [3, с. 172].

Отже, зазначимо, що фактичний час здійснення електронно-обчислювальних операцій та транзакцій під час здійснення банківських електронних платежів встановити можна, але у юридичному сенсі початок шахрайських дій та настання наслідків виявити складніше. Із метою отримання уявлення щодо події шахрайства, уповноважена особа повинна

проаналізувати всі місця, де відображені шахрайські дії, та час їх здійснення, довести зв'язок між діями та настанням наслідків у вигляді заволодіння грошима громадян внаслідок незаконних електронних операцій.

Із метою отримання уявлення щодо події шахрайства, уповноважена особа повинна проаналізувати обстановку, враховуючи всі місця, де відображені шахрайські дії.

С. В. Самойлов до таких відносить місцезнаходження:

– банкоматів (магазин, вулиця тощо);

– 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» тощо);

– установ, де впроваджено системи розрахунків за допомогою пластикових кредитних карток тощо [168, с. 8].

У свою чергу, Т. В. Коршикова типовими місцями вчинення шахрайств з використанням електронно-обчислювальної техніки називає: місце проживання злочинця, місце роботи, а також спеціально вибрані місця, де є доступ до мережі Інтернет, зокрема ті місця, де не встановлено відеокамери, які дають змогу зафіксувати перебування у таких місцях злочинця. До таких місць, переважно належать заклади харчування, де наявна мережа Інтернет, громадські місця, де поширено розповсюдження WI-FI, місця позбавлення волі. Зафіксовано непоодинокі випадки, коли такі шахрайства можуть вчинятися поза межами нашої держави, а також з тимчасово окупованих районів [86, с. 75].

На думку А. І. Анапольської, місцями незаконного заволодіння грошовими коштами, що перебувають на електронних рахунках у більшості випадків є робочі місця працівників підприємств, установ чи організацій (у т.ч. банків), Інтернет кафе (клуби), місця проживання злочинця, спеціально зняті квартири. За умови безпосереднього доступу до інформації про електронні рахунки, шахрайства у більшості випадків вчиняються у денний

час; при опосередкованому доступі до інформації про електронні рахунки, шахрайства найчастіше вчиняються в вечорі [7].

За результатами аналізу матеріалів судово-слідчої практики [Додаток А] та опитування респондентів [Додаток Б], місцями вчинення шахрайства у сфері банківських електронних платежів, можуть бути:

– місця знаходження комп'ютерної техніки, з якої здійснюються шахрайські дії (стаціонарне комп'ютерне обладнання, ноутбук (телефон, планшет), що переміщується у просторі і підключений до мережі Інтернет) (29 %);

– місця знаходження банкоматів, банків, в яких знімалася готівка (18 %);

– місце знаходження потерпілого, який виявив шахрайські дії при здійсненні електронних платежів (22 %) тощо [Додаток А, Б].

Часові параметри є достатньо розпливчасті, втім часом вчинення шахрайства у сфері електронних банківських платежів вважаємо момент проведення транзакції, завдяки якій потерпілого було позбавлено грошей на його рахунку.

У криміналістичній літературі справедливо підкреслюється необхідність врахування у криміналістичній характеристиці кримінального правопорушення даних про сліди.

Адже вивчення слідів дозволяє визначити спосіб та механізм учинення злочину, спосіб його приховання, особу злочинця, а також встановити ряд обставин під час розслідування злочину, викрити неправдиві показання свідка або злочинця, приховані ним речові докази злочину тощо [192, с. 106].

Прихильниками класичного підходу, що містить у собі єдність матеріальних та ідеальних слідів злочину, є М. В. Салтевський та інші вчені [160, с. 149]. Натомість, за результатами емпіричних досліджень та аналіз криміналістичної літератури, механізм слідоутворення під час вчиненні шахрайства у сфері банківських електронних платежів доволі специфічний, адже ряд операцій здійснюється у віртуальному форматі.

На цьому наголошує й О. А. Самойленко, яка стверджує, що використання кіберпростору для вчинення традиційного злочину суттєво детермінує механізм його вчинення. Застосування технологій кіберпростору (телекомунікаційних мереж, комп'ютерних систем й пристроїв), як знарядь досягнення протиправної мети призводить до утворення специфічних змін (слідів в криміналістичному сенсі) у самому кіберпросторі як інформаційному просторі взаємодії людей [163, с. 76].

Отже, із появою нових можливостей здійснення фінансових операцій за допомогою різних технологій – Інтернет, мобільних, безконтактних пристроїв, спеціальних програмних додатків, набувають особливого значення віртуальні сліди [215, с. 5]. При цьому, сліди вчинення даних злочинів рідко залишаються у вигляді видимих змін навколишнього середовища. Вони в основному не розглядаються сучасною трасологією, оскільки в більшості випадків носять інформаційний характер, тобто є тими або іншими змінами в комп'ютерній інформації, що виражається у формі її блокування, копіювання, модифікації, знищення. Скоєння особою протиправних дій, пов'язаних із використанням комп'ютерних технологій спричиняє виникнення певної кількості слідів у тому числі і специфічних, притаманних лише зазначеній категорії злочинів. Використання цих інформаційних даних при розслідуванні злочинів є необхідною умовою забезпечення всебічного, повного й об'єктивного дослідження обставин справи [39, с. 263].

Отже, слід погодитися із А. С. Білоусовим, що необхідність виокремлення слідів такого роду в самостійну групу як окремих об'єктів пов'язана з особливістю протиправних дій з комп'ютерною інформацією, що полягає в тому, що місце вчинення безпосередніх протиправних дій і місце, де наступають наслідки злочину і де вони можуть бути виявлені, можуть перебувати на досить таки великій відстані одне від одного [18, с. 9]. Підтримують необхідність доповнення класичної класифікації слідів групою віртуальних слідів й В. О. Давидов та А. Ю. Головін, які під останніми розуміють зафіксовану у вигляді цифрового способу формальної моделі

зміну стану інформації в пам’яті абонентських електронних пристроїв (терміналів, білінгових систем тощо), викликану алгоритмом встановленого програмного забезпечення і пов’язану з подією злочину (що має кримінально-релевантне значення) [34, с. 254].

Робимо висновок, що віртуальні сліди (їх ще називають електронно-цифрові) є проміжним явищем між традиційними матеріальними та ідеальними слідами, адже процес передачі інформації, що полягає у передачі електронно-цифрового коду, здійснюється завдяки матеріальним носіям (комп’ютерам, телефонам тощо). Утім, на відміну від ідеальних слідів, які залишаються у пам’яті людини, процес здійснення передачі електронної інформації залишається в пам’яті комп’ютерних та інших цифрових пристроїв.

У контексті даної проблематики слід звернути увагу на думку А. С. Білоусова, який наголошує, що віртуальні сліди існують об’єктивно на матеріальних носіях, але не доступні для безпосереднього сприйняття. Для їх сприйняття потрібне обов’язкове застосування програмно-технічних засобів, отже наявність таких слідів на матеріальному носієві наближує цю групу до матеріальних слідів, але не робить їх такими. Отримані з матеріального носія і сприйняті віртуальні сліди внутрішньо не надійні завдяки природі їх існування, тому, що їх можна неправильно прочитати, наприклад, застосувавши інші програмно-технічні засоби, легко підробити, легко втратити. Це близько до суб’єктивного сприйняття і наближає такі сліди до ідеальних, але не може бути ототожненим з останніми. Віртуальні сліди зберігаються в ідеальному вигляді, але не в пам’яті людини, а в машинній пам’яті і на матеріальних носіях машинної інформації, їх виявляють з використанням технічних засобів у відповідності до певних алгоритмів [18, с. 9].

Отже, у зв’язку із розвитком комп’ютерних технологій та поширенням системи електронних розрахунків, а також зручністю зберігання коштів

громадян на електронних рахунках, якими все частіше заволодівають шахраї, вбачається поступова зміна класичного підходу до визначення груп слідів.

Адже вчинення досліджуваних нами кримінальних правопорушень пов'язане з використанням великого різноманіття носіїв комп'ютерної інформації, що мають різну природу – пам'ять комп'ютера, лінії електрозв'язку, роздруківки матеріалів з принтера тощо, для роботи з якими потрібні різноманітні технічні засоби, а в багатьох випадках – ще й навички та спеціальні знання [18, с. 9]. Також нетрадиційні й традиційні сліди зазвичай містяться на місці підготовки до злочину (розробки вірусу, програм зламу, добору паролів) та місці (комп'ютері, сервері або стримері) обробки інформаційного продукту як предмета посягання [163, с. 132].

Досліджуючи типові сліди злочинів, вчинених у сфері функціонування електронних розрахунків, А. І. Анапольська також пропонує розподілити їх на: матеріальні сліди (сліди-відображення, сліди-речовини, сліди-предмети), ідеальні та електронні цифрові сліди. Кількість слідів, їх види та місця виявлення прямо залежать і можуть змінюватися залежно від обраного злочинцем способу готування, вчинення та приховування злочину. До електронно-цифрових слідів вчена відносить відомості (повідомлення, дані), зафіксовані на матеріальному носії та об'єктивно представлені у вигляді відображення інформації тимчасового та ідентифікаційного характеру в автоматизованих інформаційних системах, що утворюється за допомогою електромагнітної взаємодії, пов'язаної з подією злочину [7].

Зокрема, слідоутворюючим об'єктом може виступати «віртуальний» об'єкт як система команд електронно-обчислювальної техніки. Відтак, цікавою є думка А. С. Білоусова, який взагалі пропонує введення поняття віртуального слідоутворюючого об'єкта для криміналістичної класифікації слідів і таку позицію пояснює тим, що система команд ЕОМ, спрямованих на створення і модифікацію файлів, є наслідком впливу як користувача, так і технологічних процесів, що викликані апаратним або програмним забезпеченням ЕОМ без участі людини. Виникнення слідів на фізичному

рівні подання інформації викликане фізичним впливом апаратних комп'ютерних об'єктів – проходженням електричного струму, намагнічуванням або розмагнічуванням певних ділянок магнітного носія в результаті дій злочинця. Ці сліди невидимі, зовнішнього прояву на апаратних елементах комп'ютерних об'єктів вони не мають. Виявити й зафіксувати, а так само вилучити й дослідити їх можна тільки з застосуванням комп'ютерних апаратних пристроїв та програмних засобів. З криміналістичної точки зору значний інтерес викликає розгляд механізму слідоутворення на логічному рівні надання інформації. Логічний рівень надання інформації є рівнем існування програмних засобів і на цьому рівні виникнення слідів викликано програмними елементами комп'ютерних об'єктів. У результаті такого впливу на слідосприймаючому об'єкті будуть відбиватися результати дії алгоритму відповідної програми або сукупності програм як слідоутворюючого об'єкта. До того ж, програмні засоби мають ту властивість, що в результаті виконання алгоритму вони також отримують відповідні сліди цього впливу [18, с. 9].

Що стосується місця події, з якого вчинялося шахрайство, то в цьому випадку йому характерна наявність наступних предметів, де можуть знаходитись сліди кримінального правопорушення:

– електронно-обчислювальна техніка (комп'ютери, їх системні блоки, ноутбуки);

– монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, джойстики тощо, 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) [86, с. 66-67].

До того ж, слід зазначити, що під час здійснення електронних банківських платежів в оперативній системі відображається час відправлення та інша цінна інформація.

Телефонні дзвінки з мобільного телефону та тексти SMS-повідомлень також автоматично фіксуються й накопичуються на сервері оператора мобільного зв’язку та можуть бути отримані слідчим [2, с. 92]. Сліди можуть міститися й у історії голосових повідомленнях та і відеодзвінках (відеододатки Skype, Google Hangouts, Zoom тощо). Втім, найцінніша інформація криється у доменній адресі (IP), що дозволяє встановити місцезнаходження точки доступу до комп’ютера, з якого здійснювалося спілкування [210, с. 74].

Виходячи із вищевикладеного та на підставі аналізу кримінальних проваджень, опитування практичних працівників можна стверджувати, що під час розслідування шахрайств у сфері електронних банківських платежів домінуюче місце займають електронно-цифрові (віртуальні) сліди, що містяться:

– у пам’яті мобільного телефону (IMEI-код; історія телефонних з’єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо) (81 %);

– на сервері мобільного оператора (25 %);

– на сервері інтернет-провайдера (сервер зберігання flow-статистики и биллінгової інформації, сервер баз даних тощо) (15 %);

– в пам’яті сім-карти (78 %);

– у пам’яті комп’ютерів, планшетів (92 %);

– у електронній поштовій скриньці (87 %);

– на флеш карті (файли, папки тощо) (79 %);

– дані електронного журналу банкомату (терміналу) (78 %);

– інформація в електронному вигляді, яка відображає суми грошових коштів, переказаних через певну систему електронних платежів («Приват-банк», «Qiwi-гаманець», MoneyGram, Western Union, Perfect Money та ін.) (61 %);

– профіль у соціальних мережах, інформація на сайтах (41 %) тощо [Додаток А, Б].

Матеріальні (44 %) та ідеальні сліди хоча і є менш поширеними, ніж віртуальні (інформаційно-цифрові), але також мають важливе значення.

Так, матеріальні сліди відображаються у квитанціях та роздруківках про електронні банківські платежі (з банкоматів, телефонів, засобів комп’ютерної техніки тощо); на банківських картках; на сім-картках; на паперових копіях комп’ютерної інформації (копії листування, скріншоти та ін.); сліди папілярних ліній на засобах комп’ютерної техніки, клавіатурі терміналу тощо.

Ідеальні сліди складають 28 % і відображаються у пам’яті потерпілих та осіб, які були свідками незаконних операцій із банківськими платежами з боку шахраїв. Отже, специфіка вчинення шахрайства у сфері електронних банківських платежів зумовлює нестандартний підхід до визначення змістовної складової обстановки та умов вчинення таких протиправних діянь, а також слідової картини, що включає себе три групи слідів: матеріальні, ідеальні та віртуальні (інформаційно-цифрові).

1.4. Характеристика особи шахрая та потерпілого

Однією з найбільш важливих складових криміналістичної характеристики шахрайства у сфері використання банківських електронних

платежів є особа шахрая. Загалом, як вказував ще у XVIII сторіччі Іммануїл Кант, для характеристики особи необхідна наявність трьох груп ознак. Автор серед них виокремив наступні: 1) задатки тваринності людини як живої субстанції, що можна підвести під загальну рубрику фізичного й суто механічного самолюбства – тобто такого, для якого не потрібно мати розум; 2) задатки людяності, які можна підвести під загальну рубрику фізичного, але порівняльного самолюбства (для чого необхідний розум), а саме схильність висновувати про себе як про щасливого або нещасного лише порівняно з іншими; 3) задатки особи як сутності істоти розумної та здатної відповідати за свої вчинки [58, с. 96]. В принципі, дані характеристики можливо застосовувати й зараз.

Розмірковуючи стосовно поняття особи злочинця наведемо окремі думки науковців щодо вказаної категорії. Так, А. Ф. Зелінський формулює вказане поняття як сукупність соціально-демографічних, психологічних та моральних характеристик, що тим чи іншим чином типово притаманні людям, винним у злочинній діяльності певного типу [53, с. 57]. Інша група науковців (Ю. В. Александров, А. П. Гель, Г. С. Семаков) зазначає, що «особа злочинця – це сукупність соціальних властивостей, ознак, зв’язків і відносин, що характеризують особу, яка порушує кримінальний закон, і в поєднанні з іншими (не особистісними) умовами й обставинами спонукають особу до антисуспільної поведінки» [4, с. 78]. Тобто бачимо, що друге визначення розширене шляхом додавання таких характеристик як зв’язки та відносини, що характеризують особу.

Отже, В. В. Бедь вказував на те, що злочинна поведінка зумовлена взаємодією особистості з соціальним середовищем. Автор наголошував на тому, що політичні, соціально-економічні, духовні сторони суспільства здійснюють зовнішній вплив на формування механізму злочину, а психічні особливості формують механізм злочину з середини. Учений робить висновок, що, крім того, вони зазначають, що психологи організованої злочинності відрізняється спільністю злочинних цілей та інтересів. До того

ж, злочинна група створюється з метою здійснення не одного єдиного кримінального правопорушення, а для постійної і довготривалої протиправної діяльності [12, с. 151].

Водночас, окрема група вчених (В. І. Курило, О. Є. Михайлов, О. С. Яра) зазначає, що кримінологічний аспект вивчення особи злочинця припускає різні «рівні» узагальнення цього поняття: конкретна особа, різні категорії злочинців, загальне поняття злочинця і містить у собі вивчення всіх зовнішніх і внутрішніх обставин, що сформували її як особу. Автори акцентують увагу на тому, що у цьому плані кримінологічний аспект найбільш широкий і містить у собі як кримінально-правовий, так і процесуальний моменти [104, с. 85-86].

Ми підтримуємо позицію В. М. Плетенця, який вважає, що вивчення особи допоможе й при протидії розслідуванню, адже у відношенні особи, до якої застосовуватиметься раптовий характер дій, у першу чергу, слід знати її соціально-демографічні, психологічні та інші дані [145, с. 242]. Тому вважаємо однією з найбільш вірних систему опису ознак особи злочинця наступними групами: 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 [189, с. 105].

Цікавою також є позиція М. Ю. Валуйської, яка вказує на можливість використання такого критерію, що має кримінально-правову природу і може рельєфно відбити внутрішньотипові структурні розходження досліджуваної сукупності, який характеризує ступінь участі особи у вчиненні кримінального правопорушення. Авторка окремими параметрами виокремлених критеріїв вказує такі: «…домінуючі інстинкти; умови соціалізації (особливо ранньої); темперамент; інтелект; вольові якості; мотивація злочину (у тому числі ступінь віддаленості від умовної психологічної норми рушійних сил конфлікту, що знайшов своє вирішення у

вчиненні вбивства); суб'єктивна кількість зусиль, докладених для досягнення злочинного результату (фізичних, інтелектуальних, психологічне навантаження з подолання психологічних бар'єрів); ступінь підготовленості вбивства» [22, с. 140]. І дійсно, у кримінальному праві особа злочинця ототожнюється із суб'єктом злочину, під яким розуміється фізична особа, тобто людина, яка є осудною, здатною під час вчинення злочину усвідомлювати свої дії (бездіяльність) і керувати ними, яка досягла віку, з якого може наставати кримінальна відповідальність [123, с. 67].

Наразі, І. М. Даньшин наголошує, що «…особа злочинця включає низку елементів, тобто певну кількість різних ознак, властивостей, рис, особливостей, що об'єднує так: соціально-демографічні ознаки (відомості про стать, вік, рівень освіти, рід занять, стаж роботи, сімейний стан, місце проживання, інші дані про соціальний статус особи). Соціально-демографічні ознаки дають істотну інформацію про особу злочинців, що може бути використана як із науковою, так і прикладною метою, зокрема під час розробки та реалізації заходів запобігання злочинам; особистісно-рольові властивості (соціальні позиції, рольові особливості тощо); соціально-психологічні якості (особливості особи, які сформувалися на базі її психічних станів і процесів у ході власного соціального досвіду; спрямованість особистості, мотиваційна сфера, потреби, установки, інтереси тощо); риси правової й моральної свідомості; кримінально-правові ознаки (спрямованість злочинної поведінки суб'єкта на конкретні суспільні відносини, узяті під охорону законом; ступінь і характер суспільної небезпечності вчиненого злочину; способи, обрані для досягнення злочинної мети; мотив, яким керувався суб'єкт злочину; ставлення винного до вчиненого) [98, с. 37–40].

Зокрема, Л. В. Сорокіна вказує, що «…слід вивчати не тільки тих, хто вже вчинив злочин, а й тих, чий спосіб життя, спілкування, погляди й орієнтації ще тільки свідчать про можливість учинення злочину. Тобто у сфері кримінологічних інтересів знаходяться також і ті особи, поведінка яких має антигромадський характер. Отже, предметом вивчення кримінології є не

тільки особа власне злочинця, а й ті, хто може стати на злочинний шлях, що вкрай важливо для боротьби зі злочинністю» [180, с. 101].

А вже В. В. Логінова вказувала на те, що особу злочинця можливо охарактеризувати за наступними групами критеріїв: «…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» [111, с. 116-118].

Цікавою є думка авторів, які вказують на те, що «…злочинці можуть класифікуватися за будь-якою демографічною ознакою (стать, вік), ознакою їх формування, соціального розвитку (освіта, спеціальність, зайнятість працею, іншими справами), соціального статусу, ролі (рід занять, сімейний стан, житлові умови, належність до соціальних груп), за безпосередніми ознаками спрямованості (потреби, інтереси, ціннісні орієнтації, вияви діяльності). Підставою класифікації осіб, які вчинили злочини, можуть бути

психофізіологічні особливості, показники фізичного або психічного здоров'я, переважання індивідуальних психологічних рис (характеру, елементів вольової та емоційної сфер). Безперечно, класифікацію особи злочинця кожна проводити за будь-якою кримінально-правовою ознакою, у тому числі за об'єктом і способом посягання, мотивом учинення тощо. За кожною з названих ознак, що є підставою класифікації, осіб, які вчинили злочини, можна поділити на відповідні групи (класи)» [108, с. 266].

Вважаємо найбільш доречним та чітким визначення особи злочинця, надане групою науковців (В. К. Лисиченко, В. І. Гончаренко, М. В. Салтевський) наголошував, що вона є досить широка, охоплює складний комплекс ознак, що його характеризують, до того ж, його моральний та духовний світ, взаємодію із соціальними та індивідуальними життєвими умовами, які певною мірою вплинули на вчинення злочину [109, с. 38].

Підводячи підсумок з цього питання, вважаємо за доцільне вказати, що особа шахрая в кримінальних провадженнях за фактом вчинення шахрайства у сфері використання 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.

Переходячи до розгляду вказаних обставин, вважаємо за потрібне привести класифікації шахраїв, надані різними науковцями. Так, окрема група вчених (П. Д. Біленчук, В. В. Кравчук, О. В. Кравчук, В. М. Кулик) виділяє дві групи злочинців: «…1) внутрішні користувачі; 2) зовнішні користувачі як суб'єкти, що звертаються до інформаційної системи як посередника, аби отримати необхідний доступ для користування інформацією. Такий підхід загалом набув підтримки багатьох криміналістів, до кола інтересів яких належить дослідження особи комп'ютерного злочинця» [16, с. 159]. В свою чергу, О. Л. Мусієнко, проаналізувавши особу

шахрая як елемент криміналістичної характеристики, визначив необхідність наявності наступних її ознак: соціально-демографічні, кримінально-правові, морально-психологічні [120, с. 14].

А вже Т. В. Охрімчук у своєму дослідженні, визначаючи відомості про особу злочинця як елемент криміналістичної характеристики та їх використання у розслідуванні шахрайства з фінансовими ресурсами, охарактеризував особу шахрая виходячи з наступних груп ознак. Зокрема, автором були відомості про властиві їм анатомічні, біологічні, психологічні й соціальні властивості, що необхідні для ідентифікації особи, вирішення тактичних завдань і установлення фактичної картини події кримінального правопорушення в процесі його розслідування [133, с. 372]. Як бачимо, критерії характеристики дещо відрізняються від запропонованих нами.

Зі свого боку, О. А. Самойленко, що з огляду на аналіз слідів вчинення шахрайства уповноважена особа може зробити висновок щодо професіонального рівня користувача як правопорушника, що зумовлене певною сукупністю ознак, зокрема: «…1) здатність злочинця використовувати технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів-анонімайзерів); 2) мобільність злочинця (індивідуальна професійна, соціальна або географічна); 3) психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети; 4) роль у складі організованої злочинної групи» [163, с. 115].

Зокрема, деякі науковці (М. І. Омельяненко, О. А. Севідов) виокремлюють своєрідні групи шахраїв. Автори аргументують такий поділ залежністю від схильності осіб застосовувати окремі способи для заволодіння майном шляхом шахрайства, учиненого з використанням ЕОТ. Зокрема, виділяються такі особи як кардери, кіберкруки, фішери, спамери, кіберсквотери та фрікери. Щодо характеристики окремих з вказаних груп, то, наприклад, О. С. Севідов зазначає, що кардери спеціалізуються на махінаціях з пластиковими картками, оплачуючи свої витрати з чужих кредитних

карток. Стосовно кіберкруків вчений зазначає, що вказані особи також займаються викраденням номерів кредитних карт з подальшим отриманням доступу до рахунків осіб, чиї номери і коди карт були викрадені [173].

А вже М. І. Омельяненко зазначає, що фішери спеціалізуються на несанкціонованому проникненні в комп'ютерні системи та мережі фінансово-банківських установ і закриті комп'ютерні системи й мережі державних силових структур та органів. Їх метою є заволодіння обманним шляхом персональними даними клієнтів онлайн-аукціонів, інтернет-магазинів, сервісів грошових переказів та іншої конфіденційної інформації. А спамери займаються масовою (понад 5-тьом адресатам) розсилкою (часто анонімних) оголошень засобами електронних комунікацій, насамперед – по електронній пошті чи в соціальних мережах. Кіберсквотери – це особи, що здійснюють захоплення доменних імен з метою наживи. Доменні імена часто називають «нерухомістю» онлайнового століття. Добре підібране ім'я може само по собі забезпечувати досить сильний потік відвідувачів, а значить, і потенційних клієнтів: вдала назва інтуїтивно перебуває й легко запам'ятовується. І наостанок, автор розкриває діяльність фрікерів, які спеціалізуються на використанні телефонних систем, зломі цифрових станцій телефонного зв'язку телефонних компаній, несанкціонованому отриманні кодів доступу до платних послуг ISDN, крадіжці й підробці телефонних карток, з метою уникнути оплати за надані телефонні послуги [128].

Цікаво О. В. Курман розкриває цей елемент криміналістичної характеристики. Зокрема, автор зазначає, що «…характеризуючи особу шахрая з фінансовими ресурсами, що це, перш за все, «білокомірцевий» тип злочинця. Такі особи вчинюють злочини без застосування насильства, з використанням неправдивих методів з метою здобуття фінансових прибутків. За своїм суспільним станом вони належать до підприємців, є професіоналами високого або середнього рівня у сфері кредитно-фінансових відношень, у більшості випадків добре орієнтуються у законодавстві – податковому, банківському, володіють знаннями в бухгалтерському обліку. У минулому

багато з них мають досвід роботи в державному секторі на посадах, пов’язаних із виконанням організаційно-розпорядчих або адміністративно-господарських обов’язків. Для особи шахрая з фінансовими ресурсами також характерно вчинення злочину як однією особою (50 %), так і групою, і, переважно, через корисливі мотиви (84,4 %). …у переважній більшості випадків шахрайство з фінансовими ресурсами вчинюють чоловіки (74,8 %) віком від 31 до 50 років (31-40 років – 41,5 %; 41-50 років – 47,4 %), які мають вищу освіту (53,3 %), займають керівні посади на підприємствах (у господарських товариствах) (69,6 %) і вчинюють злочин, як правило, у межах одного населеного пункту (88,2 %). Тривалість злочинних дій складає, у більшості випадків, – від шести місяців (16,3 %) до двох років (57 %). За цей час злочинці встигають незаконно одержати кредит або скористатися правом на пільгове оподаткування від одного до восьми раз (один раз – 50,9 %; два рази – 20 %; три – 13,6 %; п’ять разів – 6,4 %; шість – 4,6 %; вісім – 2,7 %)» [106, с. 8].

Отже, почнемо виклад власного дослідження. Так, на підставі аналізу кримінальних проваджень [Додаток А] визначено, що шахрайства в сфері банківських електронних платежів, переважно вчиняють чоловіки – 79 %. Дану статистику можна роз’яснити більш високим рівнем соціальної активності чоловіків.

Така характеристика як вік особи є обов’язковою позицією у протоколах допиту підозрюваного та у повідомленні про підозру, і, про що говорить аналіз кримінальних проваджень [Додаток А], досліджуваний вид шахрайства вчинюється у такому віці: на момент вчинення протиправного діяння шахраї перебували у віці 18-25 років (35 %), 25-35 років (44 %), 35-45 (17 %), 45 років і старше (9 %). Отже, найбільш криміногенну групу складають особи віком 25-35 років.

Залежно від рівня освіти шахраїв з’ясовано [Додаток А], що базову середню освіту має 1 %, середню – 1 %, середню спеціальну - 6 %, базову вищу – 19 %, вищу – 73 %.

Як зазначає певна група науковців (М. І. Стрюк, С. О. Семеріков, А. М. Стрюк), «…у кіберпросторі злочинець-користувач може бути суб'єктом багатьох соціальних спільнот (груп) у соціальних мережах, мати багато активних акаунтів (з англ. account) чи профілів, облікових записів, або ж узагалі не мати потреби в цьому. Варто додати, що географічна мобільність не завжди пов'язана з професійною, адже людина може мати високий ступінь географічної мобільності без можливості змінити особистий вибір і компетентність (роз'їзна робота з низьким рівнем професійної, соціальної та економічної мобільності)» [186, с. 44]. Тобто рівень освіти впливає, звичайно, і на професійний стан особи шахрая. Так, щодо професійної зайнятості [Додаток А] було зроблено висновок, що переважна більшість шахраїв (61 %) працювали у сфері підприємницької діяльності та сфері комп'ютерних технологій.

Стосовно соціального статусу необхідно вказати, що, як показує аналіз судово-слідчої практики [Додаток А], більшість з них неодружені (67 %). Під час учинення шахрайських дій лише 1 % правопорушників знаходився у стані сп'яніння.

Доречною вважаємо позицію О. А. Самойленко, у якій запропоновано правопорушників, які вчиняють протиправне діяння із застосуванням становища кіберпростору, розділити на п'ять типів: 1) злочинець – користувач початкового рівня; 2) злочинець – користувач; 3) злочинець – упевнений користувач; 4) злочинець – досвідчений користувач; 5) злочинець – користувач професіонал. Авторка робить висновок, що злочинець – користувач початкового рівня з урахуванням своїх професійних навичок роботи з комп'ютером не використовує технології анонімізації доступу до ресурсів Інтернет; характеризується високою соціальною мобільністю з різних причин (нереалізованість комунікаційних потреб (людина з обмеженими фізичними можливостями, наявність психічних хвороб), наявність географічної мобільності, за відсутності професійної та економічної мобільності (сезонний працівник; робота за кордоном вахтовим

методом; кур’єр; водій; сортувальник тощо, причому злочинець виконує роботи низької кваліфікації)). Підсумовуючи, науковиця зазначає, що проблеми конкуренції мотивів вчинення злочину він не має, його злочинна діяльність зазвичай становить собою елементарну вольову дію, як-от розміщення в мережі Інтернет інформації певного місту [165, с. 200]. Як бачимо, дане твердження підтверджує наші емпіричні відомості.

Достатньо цікаво К. Д. Заяць пояснює, 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, потрібно називати «елітою» серед представників кримінального світу. Автор вказує, що шахраї цієї категорії – це інтелектуально обдаровані особи, які бачать метою свого життя виявляти слабкості державної системи й законодавства, та користуватися ними для власного збагачення [51, с. 98]. З огляду на сказане, слід відмітити досить низький показник кількості раніше засуджених осіб – лише 5 % [Додаток А].

Також було з’ясовано [Додаток А], що даний вид шахрайства здійснюють як ОГ та ЗО (23 %), так й окремі особи (77 %). Організатор групи безпосередньо управляє її діяльністю.

Також в розрізі зазначеного варто привести думку О. А. Самойленко, яка відмітила, що «…технологія «хмарних обчислень» і децентралізованих мереж обміну інформацією та засобів зберігання означає, що, незважаючи на можливість ідентифікації місця перебування конкретного засобу комп’ютерної техніки в конкретний момент часу, аналогічні дані можуть існувати у вигляді декількох копій, розповсюджуватися між багатьма пристроями й місцями знаходження та переміщуватися в інший географічний локус за декілька секунд. Організовані злочинні групи використовуватимуть саме такі технології, оскільки останні справляють безпосередній уплив як на вчинення злочину, так і на процес його розслідування. По-перше, якщо постачальник Інтернет-послуг або безпосередньо відомості перебуватимуть поза межами юрисдикції державних органів країни, в якій проводиться

розслідування, процес розслідування такої злочинної діяльності буде ускладнений тривалими процедурами надання взаємної правової допомоги. По-друге, інформація в децентралізованих комп'ютерних мережах досить часто є зашифрованою або фрагментованою, це змушує правоохоронні органи звертатися по допомогу до відповідних фахівців, застосовувати заходи примусу відносно постачальників послуг або фізичних осіб, що ускладнює доступ до екстериторіальних джерел інформації» [162, с. 410].

За результатами узагальнення даних кримінальних проваджень [Додаток А], 71 % осіб, які вчиняють шахрайства в сфері банківських електронних платежів, відрізняються досить високим рівнем інтелекту та посідають авторитетне місце у суспільстві.

Підсумовуючи, зазначимо, що шахрайства досліджуваного виду 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.

Стосовно особи потерпілого, для початку приведемо позицію О. В. Кравченко, який зазначав, 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, що склалась, обидві сторони діють згідно з особливостями своїх інтересів і поглядів, які нерідко в них співпадають [90].

Поняття потерпілого міститься у ч. 1 ст. 49 КПК України: «Потерпілим визнається особа, якій злочином заподіяно моральну, фізичну або майнову шкоду» [97]. Найчастіше від дій шахраїв страждає особа, яка виступає набувачем товарів та послуг (покупець). До того ж, покупці на електронному ринку дещо відрізняються від покупців на традиційних фізичних ринках. Оскільки доступ до Інтернет пов'язаний із придбанням обладнання та наявністю певного рівня освіти, користувачі мережі характеризуються

вищим рівнем доходів та освіти, ніж середній покупець на реальному ринку [42].

А вже С. В. Головкін, із огляду на проведене дослідження, наголошує на тому, 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.» [29, с. 12]

Зокрема, О. Л. Мусієнко акцентує увагу на тому, що залежно від наявності й впливу різних відносин, що існували або утворилися між шахраєм та потерпілим до вчинення кримінального правопорушення, проводиться розділення зв’язку за обставинами його утворення. Автор наголошує, що зв’язок за обставинами його утворення є залежним від наявності й впливу різних соціальних відносин, що існували або утворилися між злочинцем і потерпілим до або в момент вчинення кримінального правопорушення, і характеру їх розвитку. Науковець, як висновок, зазначає, 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» [121, с. 83–85].

Також С. В. Чучко зазначає, що потерпілими від шахрайства «…можуть виступати будь-які фізичні особи, підприємці, інші споживачі товарів та послуг. Утім, 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» [210, с. 92]. Дійсно, це наявна проблема, яка потребує нагального вирішення.

Актуальною наразі є позиція С. В. Самойлова, який зазначає, що для дослідження особи потерпілого усіх потерпілих поділено на дві категорії: 1) активних користувачів мережі, які постраждали внаслідок недобросовісного виконання обов'язків за договором купівлі/продажу (обміну); 2) користувачів, які мають невеликий досвід використання мережі та стали потерпілими внаслідок відсутності необхідних знань про заходи обережності в мережі «Інтернет». Автор наголошує, що серед потерпілих обох категорій наявні особи, які навмисно порушують вітчизняне законодавство чи законодавство інших країн [168, с. 8]. Як бачимо, поділ на відповідні групи має місце в науковій літературі.

А вже Л. В. Франк стверджує, що специфічність же криміналістичного вивчення полягає в тому, що його об'єктом не обов'язково є особа, визнана відповідною постановою або ухвалою потерпілим. Так, автор наголошує, що віктимологічні дослідження не можуть обмежуватися дослідженням лише

тих осіб, які визнані потерпілими компетентними органами. Адже зв'язок потерпілого та злочинця не є однотипним. Тут можна виділити різні рівні, різноманітні типи зв'язку злочинця і його жертв. Як висновок, вчений вказує на те, що деталізація суб'єктивного зв'язку між потерпілим і злочинцем має бути багатоступінчастою, повинні бути уточнені найтонші перехідні грані [198, с. 32].

Говорячи про зв'язки потерпілого та злочинця вважаємо за доцільне звернутися до дослідження О. Л. Мусієнка. Автор зазначає, що зв'язок «злочинець–потерпілий» може утворюватися й при відсутності спеціального пошуку або вибору жертви злочинцем, при відсутності відповідних пошукових дій жертви й взаємного співробітництва цих двох осіб. У подібних випадках конкретна особа стає жертвою найчастіше при випадкових обставинах. На думку вченого, випадковий характер утворення зв'язку при відсутності або незначних даних про обставини зустрічі шахрая і його жертви створює певні труднощі для розкриття злочину й встановлення винної особи. У цьому випадку важливо простежити лінію поведінки потерпілого перед посяганням, урахувати й перевірити всі можливі його зустрічі, виявити очевидців та інших свідків, які можуть повідомити необхідні відомості, ретельно дослідити обстановку місця події. О. Л. Мусієнко робить висновок, що критерії, які лежать в основі типології зв'язку «потерпілий-злочинець», одночасно характеризують найбільш істотні сторони розглянутого зв'язку. Час утворення зв'язку, характер знайомства шахрая і його жертви, специфіка їхніх взаємин, спосіб утворення зв'язку – все це різні аспекти, що дозволяють одержати чітке уявлення про зв'язок «злочинець-потерпілий» [118, с. 92].

На основі аналізу матеріалів кримінальних проваджень [Додаток А] було виокремлено наступні віктимогенні групи потерпілих, а саме:

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.

Підводячи підсумок, зазначимо, що особа потерпілого має важливе значення для кримінальних проваджень досліджуваної категорії. Адже в більшості випадків саме жертва обману подає заяву про вчинене протиправне діяння. Тобто ефективно проведені СРД, НСРД та інші процесуальні дії з вказаною особою будуть сприяти загалом розслідуванню шахрайства даного виду.

Висновки до розділу 1

Під час дослідження криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів необхідно зробити наступні узагальнення:

1. Визначено, що криміналістична характеристика відносно нова категорія загалом у криміналістиці та в методиці розслідування кримінальних правопорушень зокрема. Водночас вона має дуже важливе значення в розрізі безпосереднього розслідування. Отже, завдяки виокремленню в ній складових з'являється можливість для побудови криміналістичних версій на різних етапах кримінального провадження. Зокрема, наповнення окремих елементів надає відповідні переваги уповноваженій особі (слідчому, дізнавачу, прокурору) під час проведення певних СРД та НСРД. Надано авторське визначення поняття криміналістичної характеристики як інформаційної моделі групи протиправних діянь певної категорії, яка має виражені складові зі сталими кореляційними зв'язками, що можуть використовуватись на будь-якому етапі розслідування. Також було розкрито її структуру.

2. Систематизовано способи вчинення досліджуваного виду шахрайства. На основі аналізу опитування працівників правоохоронних органів встановлено, 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.

3. На основі аналізу матеріалів судово-слідчої практики та опитування респондентів визначено місця вчинення шахрайства у сфері банківських електронних платежів: місця знаходження комп'ютерної техніки, з якої здійснюються шахрайські дії (стаціонарне комп'ютерне обладнання, ноутбук

(телефон, планшет), що переміщується у просторі і підключений до мережі Інтернет) (29 %); місця знаходження банкоматів, банків, в яких знімалася готівка (18 %); місце знаходження потерпілого, який виявив шахрайські дії при здійсненні електронних платежів (22 %) тощо.

4. З'ясовано, що матеріальні сліди відображаються у квитанціях та роздруківках про електронні банківські платежі (з банкоматів, телефонів, засобів комп'ютерної техніки тощо); на банківських картках; на сім-картках; на паперових копіях комп'ютерної інформації (копії листування, скріншоти та ін.); сліди папілярних ліній на засобах комп'ютерної техніки, клавіатурі терміналу тощо. Ідеальні сліди складають 28 % і відображаються у пам'яті потерпілих та осіб, які були свідками незаконних операцій із банківськими платежами з боку шахраїв. Визначено, що специфіка вчинення шахрайства у сфері електронних банківських платежів зумовлює нестандартний підхід до визначення змістовної складової обстановки та умов вчинення таких протиправних діянь, а також слідової картини, що включає себе три групи слідів: матеріальні, ідеальні та віртуальні (інформаційно-цифрові).

5. Вважаємо за доцільне вказати, 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.

6. Виокремлено віктимогенні групи потерпілих, а саме: 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.

РОЗДІЛ 2
ОРГАНІЗАЦІЙНІ ЗАСАДИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

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

Сфера здійснення безготівкових розрахунків є невід'ємною частиною економіки України. Розвиток і вдосконалення банківських електронних платежів зіграло важливу роль в банківській справі: дозволило знизити операційні банківські витрати, розширити сегмент активних клієнтів, підвищити їх лояльність. Але також гостро стоїть проблема інформаційної та фінансової безпеки клієнтів, що користуються дистанційними видами банківського обслуговування, зокрема при роботі з банківськими електронними платежами. Перед більшістю країн, у яких активно розвиваються операції з використанням онлайн банкінгу виникають різні види загроз шахрайства, не є винятком і Україна [71, с. 98].

Як зазначає О. А. Самойленко, «…специфічність механізму вчинення злочинів у кіберпросторі, зокрема, особливості їх слідів, які можуть бути легко фальсифіковані або взагалі знищені, обумовлює й особливості початку кримінального провадження щодо цих злочинів. Тут йдеться про ті особливості, які вимагають їх врахування з точки зору забезпечення судової перспективи таких справ» [161, с. 165]. Отже, безсумнівно, користуватися безготівковим розрахунком за допомогою онлайн банкінгу набагато зручніше, ніж готівкою. Не доводиться носити з собою грошові суми, а в тих випадках, коли їх не вистачає під час розрахунку за покупку, знову ж на допомогу приходить банківська карта, по якій можливо отримати кредит

миттєво за допомогою смартфона і додатку банку. З іншого боку, всі ці зручності та переваги шахраї використовують в своїх корисливих цілях і, отримавши верифікаційні дані протиправним шляхом, можуть здійснювати різні операції, розраховуючись за їх вчинення чужим майном, тобто грошовими коштами, які їм не належать.

А вже Ю. П. Аленін акцентує увагу на тому, що процесуальний порядок, встановлений у ст. 214 КПК України, не враховує загальні положення процесуальної діяльності та національні правові традиції. Вчений наголошує, що будь-яка галузь процесуального права має передбачати попередній, перевірочний, фільтраційний етап перед основним провадженням [6, с. 201]. Тому одразу необхідно вказати, які джерела формують первинну інформацію про кримінальні правопорушення досліджуваної категорії.

Так, С. В. Самойлов серед джерел первинної інформації про правопорушення та прийняття рішення про початок кримінального провадження визначив наступні: «…1) заяви чи повідомлення представника Інтернет-сервісу, на якому було виявлено шахрайство – 15%; 2) заяви чи повідомлення від потерпілого – 85%. Поряд з тим, наголошено 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» [168, с. 8]. Тобто внесення відомостей до ЄРДР відбувається з огляду на наявність вказаних джерел.

Наразі, окрема група науковців (В. В. Вапнярчук, Ю. М. Грошевий,

В. Я. Тацій) стверджує, що «…зазначена діяльність відповідає критеріям самостійного провадження, оскільки є системою процесуальних дій у межах кримінальної процесуальної форми досудового провадження, які зумовлюють виникнення певної сукупності процесуальних відносин та спрямовані на виконання єдиного завдання, і цілком правомірним є розуміння й дослідження цієї діяльності саме як самостійного провадження» [23, с. 334].

Зокрема, О. А. Самойленко вказує на те, що у зв'язку з цим важливим є врахування наступних міркувань: «…завданням початку досудового розслідування є своєчасна реакція вповноважених державних органів на інформацію про кримінальне правопорушення (полягає в невідкладній реєстрації в ЄРДР і початку кримінального провадження) поєднана з аналізом отриманих відомостей, що можуть не утримувати ознак саме кримінального правопорушення або взагалі бути помилковими чи неправдивими; на цій стадії не лише приймаються заяви, повідомлення про вчинене кримінальне правопорушення та здійснюється їх перевірка, але й приймається обґрунтоване рішення щодо проведення досудового розслідування за іншими джерелами інформації; ця стадія не залежить від інших етапів кримінального провадження, зміст її зумовлений колом вирішуваних питань». Авторка робить висновок, що сутність стадії початку досудового розслідування виявляється в процесуальній діяльності слідчого, прокурора з розгляду первинної інформації про кримінальне правопорушення (її прийняття, реєстрація, перевірка та прийняття рішення) [163, с. 169].

Також доречною є думка С. В. Самойлова з приводу того, що наявні характерні ознаки, які виокремлено на підставі вивченого емпіричного матеріалу. Зокрема, серед них визначено такі, наявність яких у первинному матеріалі орієнтує слідчого на викриття ознак шахрайства, вчиненого саме з використанням мережі «Інтернет», зокрема: 1) факт взаємодії потерпілого та зловмисника через мережу «Інтернет»; 2) факт передачі коштів, майна чи

права на майно; 3) факт невиконання іншою стороною зобов'язань у межах домовленості [168, с. 8].

С. В. Чучко на основі аналізу матеріалів судово-слідчої практики встановив, «…що початкові відомості, які були підставою для внесення відомостей в ЄРДР за фактом учинення шахрайства при купівлі-продажу товарів через мережу Інтернет, надходили до правоохоронних органів з таких джерел: «…а) заяви, листи та повідомлення, що надійшли від громадян, які отримали інформацію про вчинене правопорушення – 91 %; в) заяви, листи й повідомлення від громадян, які стали свідками злочинної події – 3 %; г) повідомлення працівників установ й організацій – 3 %; д) матеріали слідства, виділені з інших кримінальних проваджень – 2 %; е) матеріали, отримані під час проведення НСРД та розшукових заходів – 1 %» [209, с. 305].

Інші науковці (В. С. Кузьмічов, Ю. М. Чорноус) вказують на те, що кримінальне провадження розпочинають у результаті виявлення безпосередньо слідчим іншого кримінального правопорушення під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні («ініціативна форма»). Автори зазначають, що традиційно діяльність з розслідування злочинів є специфічним видом соціальної практики, що полягає в пізнанні подій протиправного характеру за допомогою передбачених законом засобів і прийомів, з-поміж яких і примусова реалізація їх у разі чинення протидії [102, с. 147]. І дійсно, такі форми можуть функціонувати в досліджуваній категорії проваджень.

У питанні визначення джерел первинної інформації, вважаємо доречним привести позицію О. Л. Мусієнко з приводу тактичних операцій, що можуть виникнути при розслідуванні шахрайства, а саме: «Затримання шахрая (групи шахраїв) на місці злочину», «Встановлення кола жертв шахрайського посягання», «Встановлення способу вчинення шахрайства», «Встановлення особи шахрая», «Документ», «Визначення розміру

матеріальних збитків» [120, с. 15].

Отже, на основі аналізу матеріалів кримінальних проваджень [Додаток А] доходимо висновку, що первинна інформація, яка була підставою для внесення даних до ЄРДР за фактом учинення шахрайства у сфері банківських електронних платежів, надходили до правоохоронних органів з таких джерел:

а) заяви, листи та повідомлення, що надійшли від громадян, які є потерпілими від визначеного протиправного діяння – 77 %;

б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене правопорушення або стали його свідками – 13 %;

в) повідомлення працівників установ, підприємств та організацій – 4 %;

г) матеріали слідства, виділені з інших кримінальних проваджень – 1 %;

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

Із початком всесвітньої пандемії COVID-19 грошові відносини громадян усіх країн зазнали докорінних змін. Зважаючи на те, що уряди багатьох країн час від часу в непередбачуваний момент запроваджують карантинні обмеження, такі як заборона роботи розважальних закладів, навчальних закладів, закладів харчування, крамниць, людство фактично адаптувалося працювати онлайн, проводити навчальний процес у вигляді онлайн-конференцій, служби доставки їжі в один момент витіснили ресторанний бізнес, практично всі магазини вимушено змінили концепцію роботи, віддавши перевагу торгівлі через сайти і соціальні мережі. Ця ситуація миттєво примусила і, як наслідок, мимоволі суттєво збільшила довіру суспільства до інтернет-банкінгу, сайтів онлайн-оплати послуг і товарів, збільшивши лояльність суспільства до сфери використання банківських електронних платежів, зробивши її частиною нормальних грошових відносин. Таким чином, пропорційно зростанню онлайн-транзакцій, збільшується і шахрайство у сфері банківських електронних платежів.

Існують різні точки зору про зміст обставин, що підлягають встановленню. Зокрема, вони передбачені ст. 91 КПК України. Таким чином, у кримінальному проваджені підлягають доказуванню: 1) подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення); 2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення; 3) вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат; 4) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження; 5) обставини, що є підставою для звільнення від кримінальної відповідальності або покарання; 6) обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення; 7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру [97]. Обставини, викладені у даній статті, являються узагальнюючими для всіх видів кримінальних проваджень, і в теорії доказів дані обставини називаються загальним предметом доказування на всіх етапах кримінального провадження. Заразом уособлення предмета доказування у кожному окремому провадженні здійснюється зважаючи на вимоги диспозиції статті КК України, за якою кваліфікується дане правопорушення, що підлягає встановленню [73, с. 146].

Відповідно до Закону України «Про електронну комерцію» електронний договір вважається укладеним з моменту одержання особою, яка направила пропозицію укласти такий договір, відповіді про прийняття цієї пропозиції в порядку, визначеному частиною шостою цієї статті. До того ж, місцем укладення електронного договору є місцезнаходження юридичної особи або місце фактичного проживання фізичної особи, яка є продавцем (виконавцем, постачальником) товарів, робіт, послуг. Момент виконання продавцем обов'язку передати покупцеві товар визначається згідно з положеннями Цивільного кодексу України про купівлю-продаж, якщо інше не встановлено цим Законом [148]. Тобто місце знаходження особи визначається наступним чином згідно чинного законодавства.

Розслідування шахрайств, вчинених з використанням електронних платежів, залишається досить складним завданням для більшості співробітників органів слідства, що обумовлено специфікою даного роду правопорушень. На практиці складнощі виникають через відсутність теоретичних методик і досвіду розслідування таких справ у співробітників правоохоронних органів. Ситуація ускладнюється також тим, що багато дрібних випадків просто не доходять до правоохоронних органів.

Шахрайства, скоєні у сфері використання банківських електронних платежів характеризуються наступним рядом специфічних ознак:

1) використання сучасних технологій для видобутку та розповсюдження платіжної інформації та персональних даних потерпілих;

2) високий професіоналізм шахраїв, деякі з яких, можливо, мають спеціальну технічну освіту;

3) велика географія шахрайства та його наслідків (наприклад, заподіяння шкоди можливе банку або фізичній особі – власнику розрахункового рахунку, який знаходиться на території іншого регіону і навіть держави);

4) безперервний процес винаходу нових способів протиправних дій із проведенням банківських електронних платежів;

5) високий ступінь організованості учасників протиправної діяльності, що істотно розширює предмет доказування у кримінальному провадженню та інші ознаки;

6) труднощі з узагальненням матеріалів слідчої та судової практики по даному виду кримінального правопорушення.

Доречною вважаємо позицію Т. В. Охрімчук, яка зазначала, що у випадку виявлення ознак шахрайства з фінансовими ресурсами необхідно встановити ряд обставин. Серед них авторка виокремлювала наступні: «…характеристика діяльності громадянина-підприємця або іншого передбаченого ст. 222 КК України суб'єкта; достовірність та обґрунтованість документів, які були надані кредитно-фінансовим установам, державним органам або іншим кредиторам з метою отримання кредиту, дотації, субсидії, субвенції, пільг щодо оподаткування; рахунки, на які були переказані від кредитора кошти; характер і зміст нормативних актів, положення яких були порушені при вчиненні злочину; осіб, причетних до вчинення злочину; наявність причинного зв'язку між діями винних осіб та їх наслідками; особливості способу вчинення злочину; визначити характер і розмір збитків, завданих кредитору; розмір несплачених податків, загальний розмір заподіяних матеріальних збитків; майно (нерухоме і рухоме), грошові кошти, необхідні для відшкодування завданих збитків; чи є в діях осіб ознаки інших злочинів; обставини, що сприяли вчиненню злочинів» [136, с. 682].

Під час розслідування шахрайства у сфері використання банківських електронних платежів можна виділити такі обставини, що підлягають встановленню: існування взаємозв'язку між способом вчинення даного виду правопорушення та механізмом викрадення коштів; місце вчинення злочину; ким вчинено шахрайство: одноосібно або групою осіб.

Слід зазначити, що також виділяються наступні обставини вчинення шахрайства з використанням електронних банківських платежів:

– використання розрахункових рахунків, що належать одному із

співучасників розкрадання грошових коштів;

– використання фіктивних розрахункових рахунків, що належать випадковим учасникам злочинного процесу;

– використання сервісів обміну грошових коштів;

– використання фіктивної юридичної особи, яка уклала договір з банком про обслуговування розрахунків з використанням електронних засобів платежу;

– переведення в готівку грошових коштів, що містяться на рахунку потерпілого, дані авторизації якого виявилися в руках зловмисників;

– оплата товарів через Інтернет з використанням персональних даних потерпілого.

Наразі С. В. Самойлов вказує, що вивчення слідчої практики дозволило визначити особливості протиправного діяння, суть яких полягає в тому, що: а) фізичне місцезнаходження шахрая, як і засобів учинення злочину, переважно не збігаються з місцем перебування потерпілого та настанням негативних наслідків злочину (місцем завдання матеріальної шкоди), а за певних випадків такі обставини можуть мати навіть транснаціональний (трансконтинентальний) характер; б) встановлено відсутність залежності пори року та інших сезонних проявів, які б прямо впливали на злочинну активність шахраїв [166, с. 99].

Як зазначав практичний працівник СБУ: «Великі атаки здійснені з серйозними напрацюваннями по вірусам типу BlackEnegry, що можна назвати кіберзброєю. Складно порахувати. Можна дивитися тільки за непрямими ознаками. Я думаю, мова йде про роботу, що коштує мільйони доларів. Ті ж типи вірусів використовуються і в інших країнах: Німеччині, США. Організація атак на Україну може йти з боку Росії. Дуже багато ознак про це свідчить. Якщо говорити про внутрішню впевненість, то вона є. Потрібно провести розслідування і отримати юридично значимі факти. У нас є з РФ договір про надання правової допомоги. Але, зі зрозумілих причин, він не працює. А значить, і неможливо в правовому сенсі до кінця розкрити

того, хто стоїть за атакою, що йде з боку Росії» [62]. Тобто уже на той час відбувалось протистояння України зі своїм східним «сусідом».

Слід розрізняти матеріальні та електронні сліди шахрайства. До матеріальних слідів у даному випадку відносяться: сліди рук, ніг, інструментів злому, як відображення зовнішнього фізичного впливу на кібернетичні системи, пристрої та мережеве обладнання; сліди тонерів, барвників, різних витратних матеріалів, що використовуються в електронних пристроях; диски, пристрої зберігання інформації, пристрої для віддаленого зняття даних та інформації, будь-якого вигляду документи та роздруківки, так звані сліди-предмети [160, с. 112].

До електронних слідів шахрайства у сфері банківських електронних платежів можна відносити: носій інформації, окремий, або інтегрований в цифрову систему, що являє собою місцезнаходження; цифровий код, що має вигляд звукового, текстового або графічного запису; обов'язкове звертання уваги на дотримання технології під час виявлення, фіксації та вилучення слідів, а також залучення фахівців, що володіють технічними, науковими та іншими специфічними навичками, використання новітніх програм та пристроїв [3, с. 173].

Під час визначення електронних носіїв інформації ми спираємося на дослідження М. В. Феоктистова. До зазначених об'єктів автор відносить різні носії, зокрема, карти пам'яті, флеш-накопичувачі, електронні ключі і т. п. Ідентифікація користувача як клієнта банку, тобто уповноваженої особи на вчинення будь-яких фінансових операцій або інших юридично значимих дій, відбувається за умови фізичного під'єднання цих пристроїв до комп'ютера [196, с. 46].

Також необхідно вказати, що має значення визначення місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів).

Зокрема, слід наголосити на засобах, що використовуються при скоєнні правопорушення: це можуть бути технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, та і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації.

Також має значення встановлення способів проникнення крізь інформаційний захист (генерація ключів і паролів, викрадення паролів, заборона доступу до облікового запису тощо).

А вже С. В. Чучко запропонував виокремити певні групи обставини, що підлягають встановленню, під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет, а саме: «…1) обставини, що стосуються події шахрайства при купівлі-продажу товарів через мережу Інтернет (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його вартості; розміщення фейкової інформації про продаж товару за умов накладного платежу з подальшим отриманням частини його вартості на платіжну карту (передоплати); створення сайтів магазинів у мережі Інтернет або їх копій, що діють за принципом фірм-одноденок; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати тощо); відомості про знаряддя (засоби) злочину; відомості про сліди злочину; відомості про предмет злочинного посягання (його кількісні та якісні характеристики), тощо); 2) обставини, що стосуються особи потерпілого та злочинця (ознаки суб’єкта злочину: фізична особа, осудність, вік, кваліфікуючі ознаки, які стосуються суб’єкта; кількість злочинців (наявність розподілу ролей серед шахраїв, функції кожного з них); 3) причинкові обставини: наявність причинного зв’язку між діями винних осіб та їх наслідками; виявлення причин та умов, які сприяли вчиненню злочину; заходи, яких необхідно вжити для їх усунення тощо; 4) решта обставин (вид і розмір шкоди, завданої кримінальним правопорушенням; кваліфікуючі ознаки щодо розміру шкоди завданої злочином; обставини, що обтяжують чи

пом’якшують покарання; обставини, що виключають кримінальну відповідальність, чи є підстава для закриття кримінального провадження; обставини, що є підставою для звільнення від кримінальної відповідальності, а також обставини, що виключають факт вчинення підозрюваною особою іншого злочину тощо» [210].

Отже, слід зазначити, що ключове значення мають також обставини, що сприяли вчиненню діяння. Не дивлячись на те, що ст. 24 ЗУ «Про захист персональних даних» передбачено, що суб’єкти відносин, пов’язаних із персональними даними, зобов’язані забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них [150], у мережі Інтернет існують різноманітні сайти-форуми, торгівельні онлайн-майданчики, де зловмисники успішно продають величезні об’єми персональних даних, здобуті злочинним шляхом, імена, адреси реєстрації, контактні дані осіб, що можуть бути використані для верифікації фіктивного клієнта банку, а також дані доступу до банківської інформації, кредитних та дебетових карток, дані доступу до онлайн-банкінгу, надають послуги створення підробних фото-ID, тощо.

Підводячи підсумок, сформуємо систему обставин, що підлягають встановленню у кримінальному провадженні за фактами вчинення шахрайства у сфері використання банківських електронних платежів, зокрема, серед них визначено наступні: 1) обставини, котрі характеризують вчинення шахрайства у сфері використання банківських електронних платежів (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: використання ботів для спаму та потрапляння шкідливих програм до комп’ютерного забезпечення потерпілого; використання реквізитів картки, що викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, з персональних комп’ютерів користувачів; відомості про сліди протиправного діяння; визначення місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного

підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); засоби, що використовуються при скоєнні правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації); 2) обставини, котрі відносяться до характеристики особи злочинця та особи потерпілого (кількість правопорушників – факт розподілу функцій серед шахраїв, завдання кожного з них); 3) причинно-наслідкові зв'язки: наявність певного зв'язку між діями винних осіб та їх результатами; з'ясування причин та умов, які сприяли вчиненню протиправного діяння; 4) обставини, що обтяжують, пом'якшують покарання чи взагалі виключають кримінальну відповідальність (чи наявні умови та підстави для закриття кримінального провадження); 5) кваліфікуючі ознаки стосовно розміру шкоди завданої протиправним діянням та обставини, котрі є підставою для звільнення від кримінальної відповідальності; 6) вид та розмір шкоди, завданої вчиненням шахрайства у сфері використання банківських електронних платежів.

2.2. Типові слідчі ситуації та відповідні їм алгоритми дій працівників правоохоронних органів під час розслідування досліджуваної категорії кримінальних правопорушень

Типові слідчі ситуації є сукупністю відомостей та інформації про злочин певного виду або групу злочинів на конкретному етапі їх розслідування. Це досить ефективна форма узагальнення відомих обставин та інформації про суспільно небезпечне діяння для його безпосереднього розкриття. Варта уваги науково-літературна класифікація та систематизація типових слідчих ситуацій надає змогу заощадити час, також практичні рекомендації щодо запобігання вчиненню подібних шахрайства у сфері банківських електронних платежів [75, с. 99].

Специфіка та безпосередня організація розслідування кримінального правопорушення, функціональні обов'язки та дії працівників органів досудового розслідування цілком залежать від кількості інформації, яка відома про подію та склад протиправного діяння, а також його учасників. Тобто, як група кримінальних правопорушень або один конкретний склад відрізняються один від одного, так відрізняються і фактичні слідчі ситуації. Типові слідчі ситуації являють собою частину криміналістичної тактики, яка, у свою чергу, є одним з чотирьох розділів системи криміналістики на ряду з загальною теорією криміналістики, криміналістичною методикою та криміналістичною технікою. Криміналістична тактика, безпосередньо як розділ криміналістики, є певною сукупністю тактичних засад, положень, норм, рекомендацій, досудового слідства, а також процесуальних дій, які є необхідними для оптимальної організації розслідування різних груп суспільно небезпечних діянь та попередження їх вчинення. Базується криміналістична тактика на нормативно-правових актах, як загального, так і спеціального характеру, на основі яких діють органи досудового розслідування.

Типові слідчі ситуації притаманні кожному кримінальному правопорушенню на етапі досудового розслідування. Вони виступають як певна сукупність оперативно-розшукових відомостей, доказів, фактів та інформації, що певним чином характерна кожному моменту (етапу) досудового розслідування в кримінальних провадженнях окремих категорій. Ці ситуації визначаються та послідовно аналізуються залежно від способу та характеру вчиненого протиправного діяння.

Принцип систематизації стосується як і приватних, так і публічних сфер життя суспільства, галузей права та створення нормативно-правових актів, адже тільки шляхом впорядкування та зведення певних норм та положень в одну систему, документ або методику можливо досягти бажаного результату виконання визначених функцій та обов'язків.

Але і в цьому напряму є певні розбіжності. Так, більшість науковців

при класифікації слідчих ситуацій беруть за основу першочерговий критерій складності: прості та складні. До того ж, слідча ситуація є складною і тоді, коли реальна інформаційна невизначеність вимагає побудови декількох її імовірнісних моделей. Якщо ж інформації про ситуацію достатньо для побудови її однозначної моделі, то така ситуація буде простою. В основі поділу лежить характеристика одного з компонентів інформаційного характеру – поінформованості слідчого [212, с. 143].

Зокрема, В. А Журавель говорить про наступний поділ слідчих ситуацій виокремлюючи серед них конфліктні та безконфліктні, що ґрунтується, на думку автора, на характеристиці одного з психологічних компонентів і зайнятої позиції учасників, а також рівні протидії розслідуванню [48, с. 157]. А вже інша група науковців (Т. О. Калюга, К. О. Чаплинський) зазначає, що «динамічність слідчих ситуацій, що змінюють свій зміст, структуру і форму в результаті впливу різних зовнішніх і внутрішніх чинників, дає підставу розрізняти серед них вихідні (з точки зору процесу розслідування), проміжні та кінцеві» [57, с. 95].

Слушною з цього приводу є думка В. К. Весельського, який акцентує увагу на тому, що в основі всіх загальноприйнятих у криміналістиці класифікацій лежить якась одна ознака. Підставою ж для загальної класифікації слідчих ситуацій є її якісна, стосовно можливості досягнення цілей розслідування, характеристика. Тому він поділяє всі слідчі ситуації на сприятливі та несприятливі для розслідування і вважає, що досягнення слідчим будь-якої з намічених цілей має починатися з оцінки наявної слідчої ситуації й, за необхідності, – з ужиття заходів щодо зміни її в сприятливу сторону [25, с. 194].

Також, залежно від наявності (відсутності) в розпорядженні правоохоронних органів інформації відносно події злочину та особи, яка його вчинила, пропонує типізувати слідчі ситуації В. М. Шевчук, який також вважає, що типізувати слідчу ситуацію доцільно за одним із основних компонентів. Автор вказує, що, зазвичай, така умова обирається наявністю

інформації про подію злочину та її учасників. Також вчений наголошує на тому, що типовими є ті ситуації, з якими стикається слідчий на початку чи наступному етапі розслідування злочину залежно від повноти вихідних даних [212, с. 148].

Тобто, принцип систематизації типових слідчих ситуацій надалі дозволить виокремити більшу кількість слідчих версій для розслідування того чи іншого протиправного діяння та пришвидшить розумні строки проведення слідчих (розшукових) дій, що безпосередньо і буде впливати на більш швидкісне та якісне реагування оперативних співробітників Національної поліції України на факт вчиненого кримінального правопорушення та на відсоток їх розкриття.

В свою чергу, М. М. Єфімов наголошував на тому, «…що у ході розслідування слідчий ознайомлюється з великою кількістю речових доказів, документів. Означена уповноважена особа реалізує це з метою безпосереднього отримання інформації в результаті проведення оперативно-розшукових і слідчих (розшукових) дій. Враховуючи це, приймаються відповідні рішення про організацію та планування процесу розслідування злочинів, використання допомоги спеціалістів й інших підрозділів органів внутрішніх справ. Дані про обставини вчинення злочину є предметом аналізу у процесі розслідування. Сукупність зазначеної інформації, отриманої з різних джерел, становить зміст слідчої ситуації» [45, с. 145].

Необхідно зупинитися на одному з найпоширеніших злочинів сьогодення, яким є шахрайство, що характеризується певною послідовністю дій суб’єкта злочину, яка спрямована на заволодіння чужим майном незаконними шляхами, застосовуючи обман, зловживання довірою та різного роду шахрайські методи. Щодо видів шахрайства:

– у торгівлі (обрахунок, обважування);

– у фінансах (фінансова піраміда, підроблені авізо);

– у будівництві (підробка документів, «купівля повітря», інвестуванням недобросовісних забудовників або підрядників);

– у стільниковому зв’язку (фрод, короткий номер);

– у мережі Інтернет (фішинг, вішинг, фармінг, клікфорд, «чарівний гаманець», «нігерійські листи»);

– у сфері банківських електронних платежів («чисте шахрайство», крадіжка персональних даних, «дружнє шахрайство», торговий фрод, міжнародний фрод, «партнерське шахрайство», «різні пристрої»).

За останні роки набув значної популярності досліджуваний вид шахрайства, адже зі стрімким розвитком вітчизняних та закордонних технологій, а також сфери інформаційних технологій, застосування банківських електронних платежів набуло великої популярності та постійно використовується для зручності як громадян, так і банківських установ. Такий спосіб платежів створений для максимальної прозорості комерційної сфери як для самого покупця, так для і продавця, але таким чином більшого поширення набули випадки шахрайства, пов’язаного з використанням електронних банківських платежів.

Статистичні дані доводять, що більш ніж 75 % від усіх збитків, заподіяних економічною злочинністю, припадає на сферу діяльності банківських установ. Згідно з проведеним аналізом найбільш криміногенними залишаються кредитно-розрахункові операції банків. Злочинні зазіхання на ресурси банків завдають збитків не лише банкам та їх клієнтам, а й негативно впливають на функціонування усієї фінансової системи держави. Більш того, банки є провідним елементом у структурі діяльності, так званих, конвертаційних центрів («конвертів»), що являють собою сукупність фіктивних та реально діючих суб`єктів підприємництва, мета яких – ухилення від податків та легалізація злочинних доходів. Діяльність зазначених структур характеризується високим рівнем латентності, злагодженою організацією учасників та складністю доказування [156, с. 12].

Проблема поширення даного виду шахрайства існує, по-перше, в системі й технічному оснащенні банківських установ, саме з точки зору

інформаційної безпеки та захисту даних, це є використання користувачами комп'ютерної техніки неліцензійного програмного забезпечення, що таким чином і використовується злочинцями, та недостатній захист комп'ютерних мереж та приватних персональних комп'ютерів.

По-друге, недостатня урегульованість нормативно-правових документів щодо вимог до захищеності систем дистанційного банківського обслуговування клієнтів. Так, багато вчених сходяться на думці, що законодавством України чітко не визначено поняття ключових термінів «кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», а лише узагальнене поняття злочинів й правопорушень, які вчиняються з використанням комп'ютерних систем та мереж.

Кіберзлочинці відчувають себе вільно не тільки завдяки низькому рівню фінансової грамотності українців, а й вельми лояльному кримінальному законодавству. В Україні шахрай при першій судимості несе відповідальність у вигляді лише штрафу. Водночас навіть ліберальний ЄС рекомендує за кібершахрайство призначати перше покарання у вигляді позбавлення волі не менш, ніж на один рік. В Іспанії за це можна отримати 12 років, в Польщі – до 25 років, в США – три-чотири довічні терміни. В Україні у 2016 р. потрапили до в'язниці лише десять шахраїв [124].

З приводу визначення поняття типової слідчої ситуації звернемось до думок науковців. Наприклад, Є. С. Хижняк вказує на те, що дана категорія, 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. Автор наголошує на тому, що на основі зіставлення типової слідчої ситуації й ситуації, що сталася під час розслідування конкретного злочину, використовуючи взаємозв'язки між елементами криміналістичної характеристики цієї групи злочинів, слідчий

зможе оптимально спланувати процес розслідування та найефективніше вирішити завдання встановлення особи, яка вчинила злочин [201, с. 197].

А вже В. В. Лисенко акцентує увагу на тому, що дослідження слідчих ситуацій сприяє конкретизації методик розслідування, підвищенню їх ролі та наближенню теоретичних досліджень до вимог практичної діяльності [110, с. 76-77]. Загалом про процес розслідування, а конкретніше про його початковий етап, доречною вважаємо думку вчених-криміналістів, які вказують, що він, як правило, характеризується невизначеністю, пов'язаною з браком інформації та її неповнотою, тому домінуючим напрямом діяльності слідчого на цьому етапі є виявлення необхідної доказової і тактичної інформації та її носіїв (джерел). О. В. Узунова та К. В. Калюга вказують на те, що це завдання вирішується з урахуванням слідчої ситуації, що складається, шляхом проведення комплексу слідчих, інших процесуальних і організаційних дій. Автори вважають, що найчастіше підставою для провадження слідчих дій є криміналістична версія, а основним завданням початкового етапу – є встановлення особи, причетної до вчинення злочину. З огляду на зазначене, вчені зробили висновок, що збирання інформації про неї розпочинається з ретроспективного вивчення слідів, залишених на місці злочину, у пам'яті очевидців, тощо. В той же час, отримана інформація використовується для висунення версій про суб'єкта злочину, визначення напряму його пошуку [195].

З приводу безпосереднього поняття слідчої ситуації, Р. Л. Степанюк вказував, що зазначена категорія може бути визначена як сформульована на підставі аналізу практики розслідування певної категорії злочинів абстрагована штучна модель, яка відображає стан наявної у слідчого інформації про обставини злочину й обставини, що склалися на відповідному етапі розслідування [185, с. 111]. А вже В. К. Весельський зазначав, що слідча ситуація належить до кола понять криміналістичної тактики і вже в цій якості, як і інші тактико-криміналістичні поняття, реалізується в криміналістичній методиці. Автор сформував перелік об'єктивних та

суб'єктивних чинників, які формують вказані ситуації. Зокрема, до об'єктивних чинників вчений відніс наступні: «…наявність і характер доказової та орієнтуючої інформації, яка є в розпорядження слідчого; наявність і стійкість існування ще не використаних джерел доказової інформації та надійних каналів надходження орієнтуючої інформації; інтенсивність процесів зникнення доказів і сила чинників, які впливають на ці процеси; наявність у даний момент у розпорядженні слідчого необхідних сил, засобів, часу і можливість їх оптимально використання; існуюча в даний момент кримінально-правова оцінка розслідуваної події». Суб'єктивними чинниками, на думку автора, є: «…психологічний стан осіб, які фігурують у розслідуваній справі; психологічний стан слідчого, рівень його знань і вмінь, практичний досвід, здатність приймати і реалізовувати рішення в екстремальних умовах; протидія встановленню істини з боку злочинця та його зв'язків, а іноді потерпілого та свідків; сприятливий (безконфліктний) перебіг розслідування; зусилля слідчого, спрямовані на зміну слідчої ситуації в бажану сторону; наслідки помилкових дій слідчого, оперативного працівника, експерта; наслідки розголошення даних досудового слідства; непередбачені дії потерпілого або осіб, не причетних до розслідування» [25, с. 194-195]. Зі свого боку, окрема група науковців (В. В. Зарубей, О. В. Ілляшенко) акцентувала увагу на тому, що підставами для висунення типових версій можуть слугувати дані щодо оперативної обстановки [50, с. 142]. Ми повністю підтримуємо зазначені позиції та вважаємо за необхідне сформулювати типові слідчі ситуації, які можуть виникнути при розслідуванні шахрайства у сфері використання банківських електронних платежів, з огляду на вказане.

На останок приведемо визначення С. С. Чернявського, який типову слідчу ситуацію формулює як інформаційну модель з найбільш значущими властивостями та ознаками процесу розслідування в кримінальних провадженнях щодо злочинів певної категорії [206, с. 405]. З огляду на зазначені визначення та позиції вчених, спробуємо сформулювати власне

авторське визначення досліджуваної категорії.

Отже, типова слідча ситуація – це сформована на підставі аналізу практики розслідування певної категорії кримінальних правопорушень інформаційна модель з найбільш значущими властивостями та ознаками певної категорії кримінальних проваджень.

З приводу класифікації типових слідчих ситуацій також наведемо думки окремих науковців. Так, С. В. Самойлов виокремлював серед них наступні: «…1) виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця або встановлено, або достатньо даних для її встановлення; 2) виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено, однак є певні відомості, що можуть вказувати на неї; 3) виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї [168, с. 9].

А вже Л. В. Борисова за результатами аналізу типових (найпоширеніших) обставин вчинення протиправних діянь досліджуваної категорії виокремлювала наступні ситуації на початковому та наступному етапах розслідування: «…1) встановлено час несанкціонованого доступу до комп’ютерної інформації, однак немає відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння; 2) встановлені час і місце несанкціонованого доступу до комп’ютерної інформації, проте особи, які володіють необхідними професійними знаннями, заперечують свою причетність до злочину; 3) встановлено час несанкціонованого доступу до комп’ютерної інформації, відома особа (особи), яка зацікавлена в цій інформації; бракує відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння; 4) встановлено час несанкціонованого доступу до комп’ютерної інформації; є сліди, що вказують на конкретного підозрюваного, але він заперечує свою причетність до вчиненого злочину; 5) визначено місце злочинного заволодіння комп’ютерною інформацією, для здійснення якого використовували механічний вплив; немає відомостей про

особу (осіб), яка вчинила це діяння» [20, с. 70].

В свою чергу, Н. О. Опанасенко на основі вивчення матеріалів кримінальних справ та проваджень за результатами розслідування шахрайства, вчиненого організованою злочинною групою у сфері житлового будівництва, встановив, що на початковому етапі виникають наступні слідчі ситуації: «…1) мала місце подія шахрайства і встановлено членів організованої групи шахраїв, які затримані в якості підозрюваних; 2) мала місце подія шахрайства і встановлено членів організованої групи шахраїв, які зникли після заволодіння грошовими коштами інвесторів» [129, с. 114-116].

Зі свого боку, Т. В. Коршикова зробила вивід, що існують дві типові слідчі ситуації. На думку авторки, перша з них має такий вигляд – встановлено факт шахрайства з використанням ЕОТ, є первинна інформація про особу (групу осіб), які можуть бути причетні до вчинення цього кримінального правопорушення або особу злочинця встановлено чи є достатньо даних для її встановлення. Другу типову слідчу ситуацію авторка формулює наступним чином – встановлено факт шахрайства з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї [88, с. 129].

В розрізі вищезазначеного, слід привести позицію О. Л. Мусієнко, який приводе наступну загальну класифікацію слідчих ситуацій, пов’язаних з окремими етапами розслідування шахрайства, прийняттям процесуальних і тактичних рішень, а саме: «…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» [121, с. 104]. Тобто вказані ситуації випливають із загального процесу розслідування.

А вже О. В. Курман говорить про те, що усі слідчі ситуації у справах про шахрайство з фінансовими ресурсами доцільно розділити на дві основні групи від обсягу та змісту даних, що слугують основою для порушення кримінальної справи та інформації про злочинця. В даному розрізі автор виокремлює наступні ситуації: «…1) слідча ситуація, що характеризується наявністю даних про вчинення шахрайство 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» [106, с. 10]. Як бачимо, О. В. Курман розділив першу ситуацію на три підвиди, що, на нашу думку, може мати місце при розслідуванні шахрайства з фінансовими ресурсами.

В свою чергу, С. В. Чучко на основі аналізу судово-слідчої практики сформулював типові слідчі ситуації розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет, зокрема: «…1) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, наявна особистісна доказова інформація, злочинець відомий – 34 %; 2) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, наявна особистісна доказова інформація, злочинець невідомий – 41 %; 3) вчинено шахрайські дії при купівлі-продажу товарів через мережу Інтернет, наявна матеріальна та особистісна доказова інформація, злочинець невідомий – 17 %; 4) вчинено

шахрайські дії при купівлі-продажу товарів через мережу Інтернет, відсутня достатня доказова інформація – 8 %» [210, с. 128]. В майже такому ж стилі сформувала перелік слідчих ситуацій О. А. Самойленко. Так, авторка за результатами узагальнення матеріалів слідчо-судової практики розслідування злочинів, вчинених у кіберпросторі, виокремила три групи типових слідчих ситуацій початкового етапу розслідування, а саме: «…1) ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця; 2) ситуації, що характеризуються наявністю неперсоналізованих відомостей про користувача як імовірного злочинця; 3) ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця» [163, с. 218]. Підтримуючи останні позиції також спробуємо виділити типові слідчі ситуації, які можуть виникнути при розслідуванні досліджуваної категорії протиправних діянь.

При типізації слідчих ситуацій на початкового етапу розслідування шахрайства у сфері використання банківських електронних платежів, вважаємо доцільним у їх зміст покласти дані відносно способу вчинення правопорушення та особи, яка його вчинила. На основі вивчення слідчо-судової практики нами було визначено сукупність типових слідчих ситуацій початкового етапу розслідування досліджуваного виду шахрайства, в якій виділено такі:

1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай відомий – 19 %;

2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %;

3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %;

4) вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %.

Стосовно алгоритмів дій, то у першій ситуації, коли був виявлений факт скоєння шахрайства у сфері використання банківських електронних платежів та відомо, що протиправне діяння вчинено або окремою особою, або групою осіб, одну з яких затримано на місці події в момент або безпосередньо після його вчинення, а інші шахраї зникли з місця події, або їх розташування невідоме, повинні бути вчинені наступні дії. В зазначеній ситуації напрямками розслідування буде виступати: виявлення та закріплення доказів скоєного кримінального правопорушення, встановлення особи шахрая та всіх співучасників, розміру заподіяної матеріальної шкоди, виявлення причин і умов, що сприяють вчиненню протиправного діяння. Основними напрямками розслідування в зазначеному випадку також будуть наступні: виявлення максимальної кількості відомостей, що характеризують потерпілого і шахрая, збір і фіксація доказів.

У другій ситуації, коли виявлений факт скоєння шахрайства у сфері використання банківських електронних платежів, відомі способи, ознаки його вчинення та приховування, але суб’єкта вчинення правопорушення не встановлено, необхідно здійснити наступні дії. За відсутності відомостей про особу шахрая основні напрямки розслідування полягають у: виявленні максимальної кількості відомостей, що характеризують правопорушника, визначення кола його знайомих, вивчення поведінки і способу життя. Також обов’язкове документування усіх наявних обставин правопорушення шляхом проведення слідчих (розшукових) дій (допити потерпілих, свідків, огляду електронно-обчислювальної техніки), реалізація відповідних негласних слідчих (розшукових) дій (оперативна перевірка особи на причетність до його вчинення, зняття інформації з транспортних телекомунікаційних мереж), а також здійснення окремих процесуальних заходів.

Третя ситуація більш складна, оскільки шахрай замаскував свої дії під вид законних фінансових операцій. У зв’язку з виявленим фактом скоєння протиправних дій, варто за допомогою відповідних експертиз та спеціалістів виявити факт незаконності дій вірогідних підозрюваних, встановити ознаки,

спосіб вчинення протиправного діяння та встановити інших учасників.

Четверта ситуація є однією з найбільш розповсюджених. Адже повідомлення про вчинення шахрайства даного виду надійшло від потерпілого, а шахрай невідомий. Отже, треба упевнитися в тому, що дійсно мала місце подія протиправного діяння. На практиці відомі випадки, коли заявник вводить в оману правоохоронні органи, повідомляючи про правопорушення з метою інсценування або приховування слідів іншого протиправного діяння. У цій ситуації необхідно опитати заявника по суті змісту повідомлення про шахрайські дії, встановити всі можливі його обставини, зібрати інформацію про особу, яка вчинила вказані дії.

Так, в березні 2017 року до гр. Б. зателефонував невідомий їй чоловік, який по телефону представився гр. В., зареєстрував її на інтернет-сайті «Tradel2.com» і шляхом вимагання змушував її перераховувати на відкритий на її ім’я особистий рахунок персональної сторінки на даному інтернет-сайті, при цьому погрожуючи фізичною розправою. З березня по липень 2017 року за декілька платежів під впливом погроз вона поповнювала рахунок своєї персональної сторінки, та в сумі перерахувала 8592 долари США, які на її думку невідомі їй чоловіки гр. В. і гр. О. переказали з її персональної сторінки. Гр. Б. не заперечує, що у травні 2017 року на її особистий валютний рахунок із інтернет-сайту «Tradel2.com» були зараховані кошти в розмірі 400 доларів США, після чого вона здійснювала електронне листування із особою, яка представилась гр. О., якому вона добровільно надала згоду на керування своїми грошовими коштами, з метою отримання матеріальної вигоди із проведення торгів на даному інтернет-сайті, однак останній повідомив, що для вчинення даних дій необхідно проінвестувати 1500 доларів США. В подальшому вказані особи здійснювали телефонні дзвінки та продовжували вимагати поповнення сторінки на інтернет-сайті «Tradel2.com», однак у серпні 2017 року, не зважаючи на дані дзвінки, вона припинила поповнення свого особового рахунку на інтернет-сайті. 09 грудня 2017 року їй прийшло смс-повідомлення про те, що на її особистий рахунок платіжної картки

зараховано 15748 гривень. Жодну з вказаних осіб потерпіла ніколи не бачила, спілкувалася з ними тільки по телефону та за допомогою електронного листування. Однак вважає, що в результаті вчинення шахрайських дій щодо неї зазначеними особами, останні заволоділи її коштами в розмірі близько 8200 доларів США, заподіявши їй значної матеріальної шкоди [181].

Практика вказує, що серед підозрюваних (учасників технологій злочинного збагачення у сфері банківської діяльності за подібними категоріями кримінальних проваджень) дуже рідко фігурують представники банківського сектору. Хоча, досить часто, саме завдяки їх безпосередньої участі відбувається процес несанкціонованого доступу до рахунків клієнтів банку та подальшого розкрадання коштів. З цього приводу переважна більшість (82 %) опитаних нами респондентів [Додаток Б] стверджує, що на практиці довести причетність банківських службовців до подібного роду зловживань вкрай важко. Труднощі, на які посилаються опитані, викликані відсутністю методичних розробок, в яких має бути розкритий зміст злочинної діяльності працівників банку в структурі технологій злочинного збагачення, особливості розкриття та розслідування комплексу економічних злочинів у цій сфері.

З огляду на вищенаведене вважаємо за потрібне привести позицію В. В. Тищенка, який виділив задачі, що необхідно розкривати на початковому етапі розслідування будь-яких протиправних діянь: «…виявлення і фіксація доказової інформації щодо злочину, який розслідується по «гарячих слідах»; вжиття заходів для запобігання втраті доказової інформації, що міститься в слідах, документах, інших об’єктах, її своєчасне виявлення та фіксація; з’ясування й оцінка сформованої після порушення кримінальної справи слідчої ситуації; виявлення джерел інформації про розслідуваний злочин; визначення напряму розслідування і розробка плану розслідування; обрання форми і методів взаємодії з органами і службами, що здійснюють оперативно-розшукову роботу; пошук і одержання інформації про механізм і обстановку вчиненого злочину; збирання і вивчення відомостей про особистість потерпілого; пошук,

одержання й аналіз інформації про осіб, що вчинили злочин, їхній розшук і затримання [191, с. 137]. Як бачимо, всі вищеперераховані завдання ми виокремили в конкретні дії, розглядаючи алгоритми дій при реалізації типових слідчих ситуацій.

Підсумовуючи вище викладене, варто зазначити про необхідність розширення наукової літературної бази щодо класифікації типових слідчих ситуацій, що в перспективі розвантажить та якісно вплине на рівень розслідування протиправних діянь. Важливого значення набувають питання та способи по запобіганню вчиненню шахрайства в сфері використання банківських електронних платежів, задля уникнення даного виду кримінального правопорушення необхідним є встановлення новітнього технічного оснащення, набір кваліфікованих як банківських співробітників, так і співробітників правоохоронних органів, а також проведення спеціальних курсів, конкурсів та практик.

Також необхідно виходити з того, що процесуальна послідовність розслідування завжди повинна виходити з оцінки реальної слідчої ситуації. При цьому повинні враховуватися всілякі зміни в майбутньому, як в результаті реалізації наміченого плану розслідування, так і в результаті дій протилежної сторони, якщо в наявності конфліктна ситуація. Таким чином, вирішення організаційних питань, що виникають в процесі розслідування шахрайства у сфері використання банківських електронних платежів, є метою слідчих, спрямованою на запобігання вченню схожих протиправних діянь в майбутньому та їх розкриття. Також вартим уваги є ситуаційне моделювання під час розслідування шахрайств досліджуваного виду, що сприяє встановленню криміналістично значущих обставин розслідуваної події та висуненню версій. Крім того, підхід до розслідування через з’ясування «слідчої ситуації» орієнтує слідчого у виборі правильного алгоритму дій як в цілому, так і окремої СРД. Тому активна боротьба із даним проявом кіберзлочинності – це нагальна вимога часу, що потребує консолідації зусиль банківських установ, правоохоронних органів, громадських організацій та, звичайно, користувачів банківських карток.

Висновки до розділу 2

Під час дослідження організаційних основ розслідування шахрайства у сфері використання банківських електронних платежів ми дійшли наступних висновків:

1. На основі аналізу матеріалів кримінальних проваджень було встановлено, що первинна інформація, яка була підставою для внесення даних до ЄРДР за фактом учинення шахрайства у сфері банківських електронних платежів, надходили до правоохоронних органів з таких джерел: а) заяви, листи та повідомлення, що надійшли від громадян, які є потерпілими від визначеного протиправного діяння – 77 %; б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене правопорушення або стали його свідками – 13 %; в) повідомлення працівників установ, підприємств та організацій – 4 %; г) матеріали слідства, виділені з інших кримінальних проваджень – 1 %; д) матеріали, отримані під час проведення НСРД та розшукових заходів – 5 %.

2. Шахрайства, скоєні у сфері використання банківських електронних платежів характеризуються наступним рядом специфічних ознак: 1) використання сучасних технологій для видобутку і розповсюдження платіжної інформації та персональних даних потерпілих; 2) високий професіоналізм шахраїв, деякі з яких, можливо, мають спеціальну технічну освіту; 3) велика географія шахрайства та його наслідків (наприклад, заподіяння шкоди можливе банку або фізичній особі – власнику розрахункового рахунку, який знаходиться на території іншого регіону і навіть держави); 4) безперервний процес винаходу нових способів протиправних дій з проведенням банківських електронних платежів; 5) високий ступінь організованості учасників протиправної діяльності, що істотно розширює предмет доказування у кримінальному провадженню та інші ознаки; 6) труднощі з узагальненням матеріалів слідчої та судової практики по даному виду кримінального правопорушення.

3. Виділяються наступні обставини вчинення шахрайства з використанням електронних способів оплати: використання розрахункових рахунків, що належать одному із співучасників розкрадання грошових коштів; використання фіктивних розрахункових рахунків, що належать випадковим учасникам злочинного процесу; використання сервісів обміну грошових коштів; використання фіктивної юридичної особи, яка уклала договір з банком про обслуговування розрахунків з використанням електронних засобів платежу; переведення в готівку грошових коштів, що містяться на рахунку потерпілого, дані авторизації якого виявилися в руках зловмисників; оплата товарів через Інтернет з використанням персональних даних потерпілого.

4. З'ясовано, що типова слідча ситуація – це сформована на підставі аналізу практики розслідування певної категорії кримінальних правопорушень інформаційна модель з найбільш значущими властивостями та ознаками певної категорії кримінальних проваджень.

5. На основі вивчення слідчо-судової практики було визначено сукупність типових слідчих ситуацій початкового етапу розслідування досліджуваного виду шахрайства, в якій виділено такі: 1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай відомий – 19 %; 2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %; 3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %; 4) вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %.

РОЗДІЛ 3
ОСОБЛИВОСТІ ТАКТИКИ ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

3.1. Організація і тактика проведення окремих слідчих (розшукових) дій

Під час розслідування шахрайства у сфері використання банківських електронних платежів проводиться ряд СРД. Серед усього переліку вказаних процесуальних дій окремі мають найбільш важливе значення.

Так, О. Л. Мусієнко за результатами анкетування та інтерв'ювання слідчих МВС України встановив, що при розслідуванні шахрайства були проведені наступні СРД: огляд місця події (62 %), слідчий огляд документів (42 %), освідування (2 %), допит свідка (98 %), допит підозрюваного (64 %), виїмка документів (34 %), виїмка предметів (24 %), обшук (38 %), призначення судових експертиз (88 %), відтворення обстановки та обставин події (16 %), пред'явлення особи для впізнання (72 %), очна ставка (28 %) [121, с. 112]. Як бачимо, в даному переліку найбільш розповсюдженими є допит свідка та підозрюваного, призначення експертиз та пред'явлення особи для впізнання.

В той же час, слід розуміти, що по досліджуваній нами категорії кримінальних правопорушень відповідні СРД можуть бути проведені, але однозначно пред'явлення для впізнання не буде таким розповсюдженим, як при розслідуванні звичайного шахрайства. Тому нами також було проведено дослідження, а саме вивчення матеріалів кримінальних проваджень за

досліджуваною категорією протиправних діянь. Як висновок, на основі аналізу зазначених матеріалів [Додаток А], мають місце наступні СРД:

– огляд місця події (59 %);

– допит потерпілого або представника потерпілої сторони (100 %);

– огляд ЕОТ, документів (85 %);

– освідування (1 %);

– допит свідка (14 %);

– допит підозрюваного (87 %);

– обшук (58 %);

– призначення судових експертиз (100 %);

– слідчий експеримент (6 %);

– пред’явлення особи для впізнання (5 %);

– одночасний допит раніше допитаних осіб (18 %).

Тобто по досліджуваній категорії кримінальних проваджень найбільш розповсюдженими СРД є допит потерпілого або представника потерпілої сторони, підозрюваного; призначення судових експертиз; огляд місця події, огляд ЕОТ, документів; обшук. Тому розглянемо саме вказані процесуальні дії.

Більшість науковців підтримують позицію, що допит є найбільш поширеним способом одержання доказів. Водночас допит – одна з найбільш складних СРД, його проведення вимагає від уповноваженої особи високої загальної й професійної культури, глибокого знання психології людини. [213, с. 218]. Так, В. О. Коновалова наголошує на тому, що допит є однією з найскладніших слідчих (розшукових) дій ще й у зв’язку з тим, що допитувані особи мають різний соціальний і професійний статус, різні особливості психіки й мотивацію своєї поведінки, що зумовлює характер спілкування, тактику проведення допиту. Вчена робить акцент з приводу того, що при цьому значна роль належить знанню закономірностей формування їх показань, що пояснюється особливостями сприйняття, запам’ятовування, відтворення, оцінювання одержаної у процесі допиту

інформації, й використання її в тактичних цілях [83, с. 3]. Вказані думки ми повністю підтримуємо та вважаємо допит, як показує вивчення матеріалів кримінальних проваджень [Додаток А], найбільш поширеною СРД під час розслідування шахрайства у сфері використання банківських електронних платежів.

Провівши аналіз кримінальних проваджень досліджуваної категорії було встановлено, допит потерпілого або представника потерпілої сторони проводиться практично у кожному випадку. Як зазначають ряд авторів – допит спрямований на встановлення безпосереднього предмета розкрадання, його кількість, види та стану, способу розкрадань чи зловживань, осіб, які брали участь у цих операціях, їх способу життя, майнового стану, оточення та іншої інформації, яка може зацікавити слідство [156, с. 19].

З приводу визначення поняття даної процесуальної дії, то ми поділяємо позицію групи науковців (В. М. Глібка, В. А. Журавля, В. Ю. Шепітька), які зазначають, що допит – це процесуальна дія, що являє собою регламентований кримінально-процесуальними нормами інформаційно-психологічний процес спілкування осіб, які беруть у ньому участь, спрямований на отримання інформації про відомі допитуваному факти, що мають значення для встановлення істини у справі [93, с. 252].

Ми підтримуємо думку О. Л. Мусієнко, який зазначив, що у цілому зміст підготовки до допиту, визначення предмета показань, черговості допиту конкретних осіб, тактики допиту залежать від сформованих слідчої ситуації розслідування й ситуації допиту, враховуються індивідуальні психологічні характеристики особи допитуваного [121, с. 122]. А вже Н. В. Павлова вказує, що у слідчого виникає необхідність ознайомлення з низкою документів, використаних під час вчинення протиправних діянь даної категорії, та відбору серед них тих, що можуть застосовуватися під час провадження допиту. Вчена акцентує увагу на тому, що з метою з’ясування картини кримінального правопорушення в цілому уповноважена особа повинна вивчити матеріали кримінального провадження та уважно

проаналізувати зміст документів, які відображають факт укладення угоди щодо відчуження житла. У зв'язку з цим уповноваженій особі необхідно звернутися до процедури укладення угоди щодо відчуження житла та її правової регламентації. На підставі вивчення матеріалів кримінального провадження та документів, що містяться в ньому, уповноважена особа повинна встановити: які дії, що вчинювалися під час укладення угоди, є незаконними, в чому вони полягають; які особи їх вчинили, коли і в якому місці; які нормативні акти, що регулюють порядок здійснення правочинів щодо житла, порушувалися тощо. Для вирішення вказаних питань вже на стадії підготовки до допиту щодо кримінальних правопорушень вказаної категорії необхідно залучити спеціалістів. Вони можуть допомогти правильно оцінити докази, роз'яснити факти, що мають значення для справи, скласти приблизний перелік питань, які необхідно з'ясувати у ході допиту [138, с. 130].

Стосовно допиту потерпілих С. В. Головкін зазначає, що це найбільш поширене джерело отримання доказів у справах про шахрайство на початковому етапі незалежно від приводів для внесення відомостей до ЄРДР. Потерпілі допитуються про обставини шахрайства, прикмети та поведінку шахраїв, маршрути їх пересування, прикмети та характеристику предметів злочинного посягання. Автор наголошує на тому, що оскільки такі особи нерідко відчувають емоційну напругу, необхідна чітка організація допиту, постановка коротких та зрозумілих питань, що виключають виникнення пауз у процесі отримання показань. Також вчений при розгляді змісту і тактики допиту потерпілих, запропонував перелік обставин, які необхідно встановити, в залежності від способу шахрайства та конкретної ситуації, що склалася в кримінальному провадженні [29, с. 11].

Загалом, вважаємо найбільш доречною позицію К. О. Чаплинського, який радить під час проведення допиту ставити питання, що стосуються таких обставин: «…виникнення злочинного задуму; відомості про об'єкт посягання, мотив злочину, ставлення особи до злочинних наслідків; способи

підготовки та вчинення злочинів, послідовність злочинних дій, а також особливості приховування злочинної діяльності (її характер); час, місце, обстановка та механізм учинення злочинів; відомості про особу злочинця; умови, за яких допитуваний спостерігав будь-які предмети або явища; психологічний та фізичний стан особи в момент сприйняття чи після нього; загальна здібність допитуваного до певного сприйняття, запам'ятовування та відтворення; обставини, що сприяли або перешкоджали учиненню злочинів; способи формування організованої групи та характер злочинної діяльності; виявлення психологічної й функціональної структури групи (якісний склад, рівень організованості) та розподілу функціональних обов'язків; кількісний склад групи при учиненні кожного епізоду злочинної діяльності, конкретні дії кожного, навички володіння зброєю та прийомами боротьби; виявлення осіб, які не брали безпосередньої участі у вчинених злочинах, але обізнаних про їх підготовку, вчинення або приховання; наявність корумпованих зв'язків та зв'язків з іншими злочинними групами; способи протидії розслідуванню та впливу на потерпілих, свідків та членів групи, які дають правдиві показання; наявність в групі конфліктів, протиріч та розбіжностей; способи легалізації отриманих прибутків та відтворення злочинної діяльності; встановлення осіб, які залишилися на волі і продовжують злочинну діяльність або налагоджують зв'язки між членами групи та намагаються створити єдину, вигідну для усіх лінію поведінки та ін.» [204, с. 210].

В свою чергу, О. Л. Мусієнко зазначає, що до нього, зокрема, можуть належати: «…з'ясування ознак (прикмет) зовнішності особи шахрая, характер його дій, дані про документи (які документи пред'являлися шахраєм, які документи оформлялися, їхній зміст, особливості оформлення тощо), відомості про дії по одержанню й відвантаженню майна, особливості майна та його вартість; відомості про порядок діяльності підприємства, порядок охорони майна та інше» [121, с. 120].

Для досягнення більшої ефективності слід заздалегідь скласти перелік питань, що підлягають з'ясуванню, це дозволить уникнути проведення повторного допиту. В ході допиту потерпілого або свідка за умови повного усвідомлення нею того, що сталося і бажанні допомогти встановленні істини використовуються наступні тактичні прийоми, розроблені в криміналістиці: бесіда, відновлення в пам'яті забутого, уточнення і деталізації показань. Як правило уповноважені особи при підготовці до допиту звертаються за допомогою до фахівців криміналістів в галузі ІТ-безпеки, яких на превеликий жаль не вистачає.

Такі кримінальні правопорушення як правило здійснюються за допомогою спеціальних програм, які маскують реальне місце знаходження особи шахрая так званих анонімайзерів таких як VPN- скорочена назва від англ. Virtual Privat Network-віртуальна приват мережа, Socks скорочена назва від англ. Socked Secure – мережевий протокол та ін. Здебільшого такі протиправні діяння вчиняються або ОГ, або ЗО.

А вже В. О. Коновалова акцентує увагу на тому, що, встановлюючи тактичні прийоми допиту та аналізуючи отримані покази, потрібно деталізувати наступні аспекти:

– умови, у яких свідок або обвинувачений спостерігав предмети і явища (удень, уночі, близько, далеко, тобто об'єктивні чинники);

– психічний стан допитуваного на момент сприйняття чи після нього (був свідок зляканий, вражений, хвилювався, знаходився в несвідомому стані, сп'янінні тощо);

– загальний стан органів почуттів людини (стан зору, органів слуху, нюху та ін.);

– загальну здатність до конкретного сприймання й запам'ятовування (зі слів допитуваного потрібно уточнити, що він краще сприймає й запам'ятовує – колір, номера, прізвища тощо) [84, с. 9].

Зі свого боку, С. В. Чучко відмічає, що «…у потерпілого від шахрайства при купівлі-продажу товарів через мережу Інтернет обов'язково

необхідно досліджувати питання стосовно наступних обставин: відповідний процес знаходження Інтернет ресурсу шахрая (рекомендація знайомих; спам-розсилка); спосіб спілкування з шахраєм (лише на сайті; на сайті і телефоном; через певні соціальні мережі); речі, які потерпілий бажав придбати; спосіб оплати» [210, с. 167]. Повністю підтримуємо зазначену позицію і вважаємо, що правильно поставлені запитання можуть бути підґрунтям для проведення подальших СРД (наприклад, пред'явлення особи для впізнання за голосом).

Підводячи висновки, зазначимо, що допит потерпілих є важливою складовою при розслідуванні шахрайства в сфері використання банківських електронних платежів, спрямований на встановлення безпосереднього предмета розкрадання. Головною проблемою є нестача відповідних фахівців криміналістів в галузі ІТ-безпеки, які б пришвидшували розкриття даних протиправних діянь, та розробляли відповідні методики для протидії [66, с. 86].

Стосовно свідків за такою категорією проваджень, то, наприклад, С. В. Головкін зазначає, що вони класифікуються на очевидців, а також осіб, яким було відомо про обставини шахрайства зі слів потерпілого та третіх осіб. Залежно від змісту отриманих даних, автор пропонує класифікувати свідків у справах про шахрайство наступним чином: 1) очевидців дій шахраїв з обману та отримання майна або права на нього; 2) обізнаних про дії шахрая в період покидання місця шахрайства; 3) обізнаних про обставини, що передували шахрайству; 4) обізнаних про факти перевезення, розвантаження, зберігання викраденого майна та інших посткримінальних дій; 5) обізнаних про факти використання викраденого майна [29, с. 11-12].

А вже О. Л. Мусієнко пропонує відносно шахрайства свідків поділити на наступні групи: «…1) особи, які тим чи іншим чином сприяли шахрайству, але самі про це не знали; 2) особи, у чиєму віданні перебувало майно (продавці магазинів, комірники, контролери, працівники бухгалтерій тощо). До цієї групи можна віднести й осіб, які виконують функції контролю або

охорони; 3) особи, чиї документи були використані при вчиненні шахрайства, але вони не мають відношення до предмета злочинного посягання; 4) особи, що не мають відношення ні до об'єкта злочину, ні до виду виробничої (чи торгової) діяльності. Ці особи виступають як свідки шахрайської діяльності (очевидці злочину); 5) особи, що перебувають у родинному чи іншому зв'язку із шахраєм; 6) особи, яким відомі будь-які інші обставини по справі» [119, с. 158].

Зі свого боку, С. В. Самойлов, на основі аналізу результатів інтерв'ювання практичних співробітників та архівних матеріалів кримінальних справ (проваджень), визначає складності у виявленні осіб, які можуть бути свідками аналізованих шахрайств. Автор встановив, що в якості таких осіб можуть бути допитані: а) особи, які вступали в подібні відносини із шахраями (були потенційними жертвами); б) співробітники групи технічної підтримки користувачів, служби безпеки сервісу чи інші особи, які відповідно до своїх службових обов'язків можуть контактувати із користувачами; в) особи, які певним чином взаємодіяли із шахраєм (співробітники служби доставки, пошти тощо); г) родичі та близькі люди потерпілого чи злочинця, які мають інформацію, що може підтвердити чи спростувати факт шахрайства [167, с. 84].

В свою чергу, Я. О. Олійник визначив наступні категорії свідків: 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 [127]. Отже,

необхідно визначити категорії свідків при розслідуванні досліджуваної категорії протиправних діянь, а саме:

– може бути відома інформація про обставини та умови протиправної діяльності, яку вони спостерігали;

– особи, які перебувають у родинному або іншому зв’язку із шахраєм;

– особи, яким відомо умови та обставини тих дій, в яких вони брали участь;

– особи, які певним чином сприяли вчиненню шахрайства, але самі про це не знали;

– особи, які були обізнані про обставини, що передували шахрайству;

– працівників банківських установ, які були задіяні в використанні банківських електронних платежів.

Допит свідків має певні особливості, адже, на що вказує О. Л. Мусієнко, обумовлені тим, що особи, у віданні яких перебувало майно, безпосередньо взаємодіє із шахраєм й більше за інших поінформовані про обставини злочину. Автор зазначає, що ці особи самі передають або беруть участь у передачі майна шахраєві. Крім того, шахрайство іноді стає можливим через неуважність або грубе порушення встановленого порядку видачі матеріальних цінностей. Обставини протиправного діяння, пов’язані з діями правопорушника відносно пред’явлення або оформлення певних документів та сприйняття зовнішнього вигляду шахрая дозволяють розширити предмет допиту свідка [121, с. 121].

Стосовно допиту підозрюваного звернемося до позиції В. Є. Богинського, який зазначає, що вказана СРД має свої процесуальні й тактичні особливості. На початку допиту підозрюваний обов’язково допитується про обставини, що стали підставою для його затримання або обрання відносно нього запобіжного заходу. В підозрюваного з’ясовується, чи визнає він себе винним у пред’явленій йому підозрі, після чого пропонується дати показання по суті пред’явленої підозри [19, с. 3].

В свою чергу, С. В. Головкін зазначає, що шахрайства на сучасному

етапі переважно вчиняються групами осіб. З урахуванням цієї обставини запропонована наступна послідовність допиту підозрюваних: спочатку – рядових членів групи, далі – лідерів. Визначені тактичні прийоми допиту обвинувачених та обставини, що підлягають встановленню, в залежності від слідчої ситуації, а також зміст і тактика очної ставки [30, с. 76].

А вже О. В. Курман розглядає тактику допиту певних осіб: директора і бухгалтера підприємства-позичальника, представників кредитно-фінансової установи, інших осіб (колег по роботі, секретарів, родичів, друзів). Автор зазначає, що особливості має також допит членів організованого злочинного угруповання, які вчинили шахрайство з фінансовими ресурсами [106, с. 11].

Зі свого боку, Т. В. Охрімчук вказує на те, що значну роль у розкритті механізму злочинної діяльності, встановленні джерел доказової інформації, викритті співучасників і конкретизації їх ролі у вчиненні шахрайства відіграє допит в якості підозрюваних головного бухгалтера, керівника суб'єкта господарської діяльності. Допит цих осіб є однією з найпоширеніших СРД у справах про шахрайство з фінансовими ресурсами. Автор наголошує на тому, що важливим завданням в організації і проведенні допиту є виконання підготовчих заходів. Вчений також характеризує особливості підготовчого етапу до проведення допиту, включаючи ознайомлення слідчого з матеріалами кримінальної справи, спеціальною літературою, нормативними документами, які регламентують порядок здійснення кредитно-фінансових операцій; розкриваються особливості вивчення особи допитуваного; доцільність залучення спеціалістів та необхідних науково-технічних засобів [134, с. 10-11].

На думку О. Л. Мусієнко, у ході допиту підозрюваного потрібно з'ясувати такі питання: «…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» [117, с. 215]. Підтримуючи наведену позицію, спробуємо сформулювати перелік питань, притаманний досліджуваній категорії проваджень. Отже, підозрюваному у вчиненні шахрайства в сфері використання банківських електронних платежів необхідно ставити наступні категорії питань:

– за яких обставин вчинено шахрайські дії;

– які способи застосовувалися (використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, які викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, з персональних комп'ютерів користувачів);

– які місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів);

– які засоби використовувалися при скоєнні правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації);

– яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчинення протиправних дій;

– який був порядок розподілу грошових коштів у членів ОГ чи ЗО;

– протягом якого періоду вчинялись протиправні діяння;

– які супутні кримінальні правопорушення було вчинено.

Підводячи підсумок, зазначимо, що допит підозрюваного необхідно проводити одразу після його затримання. Це забезпечить найбільш якісні

показання щодо факту вчинення шахрайства у сфері банківських електронних платежів.

Протягом останнього десятиріччя в Україні та в усьому світі інформаційні технології зробили великий крок вперед, внаслідок чого загострилась криміногенна ситуація. З масовою комп'ютеризацією та використанням всесвітньої мережі Інтернет актуальності набуває діяльність правоохоронних органів у боротьбі з шахрайством в сфері використання банківських електронних платежів. Кожен день у всьому світі відбуваються десятки тисяч інцидентів таких злочинів, які вчиняються в банківській сфері з використанням мережі Інтернет. Відповідно до звіту «Norton Reports 2017» збиток таких злочинів у всьому світі склав 172 млрд. доларів США, а кількість потерпілих від шахрайських операцій становить 978 мільйонів користувачів [131].

Безумовно, такі явища вимагають негайного реагування правоохоронних органів. В Україні такими кримінальними правопорушеннями займається 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 [132].

Як правило, підставою для відкриття кримінального провадження за ст. 190 КК України є заяви про несанкціонований доступ, розкрадання грошових коштів з банківських рахунків. Надходять вони, як правило, від юридичних осіб, набагато рідше від громадян. Поясненням цьому може бути те, що громадяни не бажають розголошувати в ході слідства викрадену інформацію, яка може містити таємні, інтимні та інші подробиці особистого життя.

Розслідування шахрайства у сфері використання банківських електронних платежів при проведенні СРД, спрямованих на отримання

інформації, яка знаходиться, як правило, на електронних носіях, а також проведення обшуку мають свої особливості.

Швидкий розвиток комп'ютерних технологій у всьому світі загострив криміногенну ситуацію в даній сфері. Кожного року шахрайство в сфері використання банківських електронних платежів призводить до багатомільярдних збитків, як юридичних, так і фізичних осіб всіх країн світу. Задача правоохоронних органів полягає в швидкому розслідуванні, протидії таким видам кримінальних правопорушень та підвищенні кваліфікації відповідних спеціалістів у цій галузі. В той же час, якісне проведення обшуків різних категорій дає правоохоронним органам достатню кількість доказової інформації [67, с. 387].

Обшук при розслідуванні таких кримінальних проваджень пов'язаний з отриманням доказів про спосіб вчинення протиправного діяння з використанням комп'ютерної техніки, а також з використанням всесвітньої мережі Інтернет. Головною метою проведення обшуку при розслідуванні кримінального правопорушення є виявлення та вилучення комп'ютерної техніки, на якій залишилися сліди протиправного діяння, наприклад, файли, документи, фото, та. ін.).

Ми поділяємо позицію К. О. Чаплинського з приводу заходів підготовчого етапу до проведення обшуку. Зокрема, автор серед них виокремлював наступні: «…вивчення матеріалів кримінальної справи; збирання орієнтуючої інформації про: - особу злочинця, а також членів його сім'ї, родичів і знайомих; - усі епізоди злочинної діяльності; - місця (об'єкти) обшуків; - знаряддя (засоби) злочину та предмети, що здобуті злочинним шляхом і підлягають відшуканню, та ін.; аналіз та оцінка зібраної інформації та слідчої ситуації, що склалася на певному етапі розслідування, до ухвалення рішення про проведення обшуку; прийняття (ухвалення) рішення про проведення обшуку; планування та визначення часу проведення обшуку; створення оптимальних умов для проведення даної слідчої дії; визначення та підготовка необхідних науково-технічних і транспортних засобів; вирішення

питання про застосування службово-розшукового собаки; добір необхідних учасників для проведення обшуку; визначення способу фіксації ходу та результатів обшуку; розробка заходів, що передбачають дії учасників обшуку у випадках виникнення непередбачуваних ситуацій або ускладнень; забезпечення безпеки учасників слідчої дії; складання плану проведення обшуку; проведення інструктивної наради (інструктаж) серед усіх учасників слідчої дії» [203, с. 339].

З приводу об’єктів, які необхідно вилучати в ході обшуку при розслідуванні шахрайства, вважаємо доречною позицію Н. В. Павлової, яка зазначала, що в основному об’єктами вилучення у провадженнях даної категорії є: «…реєстраційні та установчі документи установи, підприємства, організації (з метою доведення фіктивності їх діяльності, встановлення терміну існування, законності отримання та стосунку до їх видачі певних осіб тощо); документи бухгалтерського обліку та фінансової звітності, інші документи, в яких відображаються господарські операції (з метою виявлення незаконних фінансових операцій, отримання інформації про фінансовий стан установи, підприємства, організації тощо); документи, що засвідчують проведення банківських операцій (заяви на переказ готівки, видаткові касові ордери, грошові чеки, платіжні доручення тощо); правовстановлюючі документи на землю, рухоме та нерухоме майно (з метою встановлення правового зв'язку конкретного майна з його власником, відповідності цих документів встановленому зразку або навпаки – встановлення факту їх підробки тощо); документи, що посвідчують особу (з метою встановлення факту їх використання у різноманітних шахрайських схемах, факту їх підробки тощо); документи про освіту та трудовий стаж, документи про стан здоров’я, страхові документи (для встановлення факту їх використання при працевлаштуванні, отриманні соціальних пільг, виплат, страховки тощо); різноманітні договори (про туристичне обслуговування, трудові контракти, про виконання ремонтних, будівельних робіт, договори купівлі-продажу, дарування, спадкування, доручення тощо); комп’ютерна

техніка та сервісне обладнання, телефони тощо; засоби маскування, що використовувалися шахраями під час вчинення шахрайських дій; обладнання для виготовлення підроблених документів, бланків, грошових купюр тощо; записні книжки, чернетки, оголошення, в яких міститься інформація про шахрайські дії; печатки, штампи, бланки документів, які використовувалися або планувалися використовуватися для вчинення шахрайства; фотографії (жертв шахрайства, співучасників тощо); майно, що здобуте злочинним шляхом» [140, с. 286-287].

При проведенні обшуку слід виділити ряд особливостей: в першу чергу потрібно звернути на комп'ютерну техніку, що знаходиться в приміщенні, а також на стан інтернет-мережі. При огляді приміщення слід провести пошук портативних USB флеш-накопичувачів, в тому числі замаскованих. Не аби яке значення має виявлення мобільного телефону, планшету на місті проведення обшуку. Як правило, на них може знаходитись дуже важлива інформація, яка слугуватиме швидкому розслідуванню злочину. Така техніка перед вилученням повинна бути правильно упакована та опечатана.

Також важливо при проведенні обшуку до потрапляння в приміщення має відключення такого приміщення від електромережі, таким чином, така дія з боку правоохоронних органів, які проводитимуть обшук, унеможливлює швидке знищення інформації, яка знаходиться на електронних носіях. Зловмисники за допомогою мікрохвильової печі можуть знищити будь-який електронний носій за лічені секунди.

Досліджуваний вид кримінального правопорушення суттєво відрізняється від інших тим, що головною його ознакою є використання всесвітньої мережі Інтернет з залученням ЕОТ. Як правило, сліди протиправного діяння по даному виду протиправних діянь знаходяться в електронному вигляді, і для виявлення та вилучення доказової бази проводиться обшук, який у 80 % випадків є результативним [74, с. 117].

Тому, з метою визначення особливостей проведення обшуку при розслідуванні шахрайства в сфері банківських електронних платежів, а

також дослідження окремих заходів його підготовки, розглянемо низку думок вчених, що досліджували проблематику даного питання.

Зі свого боку, О. В. Білоус зазначає, що під час кримінального провадження з проникненням до житла чи іншого володіння особи здійснюються чи можуть здійснюватися: затримання особи, тимчасовий доступ до речей та документів, арешт майна, контроль за поведінкою підозрюваного, обвинуваченого, який перебуває під домашнім арештом, обшук, огляд, слідчий експеримент, обстеження публічно недоступних місць, житла чи іншого володіння [17, с. 268].

Тому при обшуку потрібно враховувати ту обставину, що його проведення найчастіше пов'язано з вторгненням в житлове чи інше приміщення, тобто ця дія обмежує деякі конституційні права громадянина. Для проведення обшуку завжди повинні бути вагомі, або, як сформульовано в законі, достатні підстави. Говорячи про достатні підстави, законодавець мав на увазі, що слідчий повинен мати інформацію, що не викликає у нього сумнівів. Така інформація отримується внаслідок проведення як слідчих (розшукових) дій, так і оперативних заходів відповідно до Закону України «Про оперативно-розшукову діяльність» [151].

А вже В. П. Головіна акцентує увагу на необхідності встановлення на початку розслідування і законності створення та функціонування юридичної особи. Авторка зазначає, що така робота відбувається шляхом дослідження портфелю документів, законності проходження процедури реєстрації та ведення фінансово-господарських операцій. Вирішити ці питання можна через проведення обшуків у підозрюваних, їх контрагентів, установах та накладення арешту на грошові рахунки підозрюваних [28, с. 119].

Аналіз матеріалів кримінальних проваджень [Додаток А] дозволив встановити, що обшук в більшості випадків проводився в місцях:

– зберігання і обробки інформації про банківські електроні платежі, що зазнала злочинного впливу (67 %);

– знаходження комп'ютерного обладнання, що використовувалося

при здійсненні протиправного діяння (43 %);

– збереження інформації, отриманої злочинним шляхом (41 %);

– настання шкідливих наслідків (10 %).

Об’єктами обшуку [Додаток А] в більшості випадків були:

– житлові приміщення (42 %);

– приміщення підприємств, організацій, установ, в т.ч. банків (37 %);

– підсобні приміщення (8 %);

– дачі (5 %);

– транспортні засоби (4 %);

– гаражі (1 %);

– інші об’єкти (3 %).

Час проведення обшуку визначається з урахуванням особливостей конкретної ситуації розслідування. Найбільшу інформативність і значимість для подальшого процесу розслідування вказана СРД набуває тоді, коли воно проводиться: а) за місцем проживання підозрюваного – в ранковий час (з 6.00 до 8.00), коли особа, у якої проводять СРД, знаходиться в непідготовленому стані, а відповідно не має можливості приховати сліди своєї протиправної діяльності; б) в організаціях, установах, підприємствах, банках – до початку робочого часу, коли комп’ютерні системи ще не задіяні в процесі проведення електронних розрахункових операцій [91, с. 150-151].

Не аби яке значення має отримання заздалегідь характеристики (плану, схеми) приміщення, в якому передбачається проведення обшуку, в бюро технічної інвентаризації або інших органах, що володіють такою інформацією. Це дозволить відразу в ході візуального огляду висунути припущення про наявність та місця можливого розташування схованок.

Також важливим при проведенні обшуку до потрапляння в приміщення є відключення такого приміщення від електромережі, таким чином, така дія з боку правоохоронних органів, які проводитимуть обшук, унеможливлює швидке знищення інформації, яка знаходиться на електронних носіях. Зловмисники за допомогою мікрохвильової печі

можуть знищити будь-який електронний носій за лічені секунди.

В свою чергу, С. В. Чучко зазначав, що на основі вивчення матеріалів судово-слідчої практики визначено, що під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет при проведенні обшуку необхідно виявляти і вилучати:

– документи, які містять відомості про можливих покупців;

– мобільні телефони, де міститься адресна книга (прізвища і адреси покупців, дані про організатора злочину), sms-повідомлення;

– комп'ютерна техніка (ноутбуки, планшети, системні блоки, флеш-накопичувачі), де може міститися інформація про протиправну діяльність шахрая. Значну увагу потрібно приділити веб-сайтам, де була розміщена інформація із послуг щодо продажу товарі [210, с. 149].

На думку В. В. Ціркаля, «…до проведення обшуку так само доцільно залучати фахівців, оскільки без їх допомоги слідчі часто виявляються безсилими в пошуку, правильному вилученні і закріпленні слідів злочину. Основними завданнями фахівців, що залучаються до процесу проведення даного обшуку, є: виконання всіх дій з комп'ютерною технікою для надання допомоги слідчому в описі комп'ютерної техніки та периферійного обладнання; проведення експрес-аналізу комп'ютерної інформації; виявлення інформаційних слідів злочинів; запобігання знищення або пошкодження комп'ютерної інформації; вилучення комп'ютерної інформації і т.д.» [202, с. 47].

Перед обранням організаційних і тактичних прийомів проведення обшуку слід вирішити низку завдань, зокрема визначити об'єкти, на які слід проводити обшук (об'єкти обшуку), предмети й документи, які потрібно вилучати (об'єкти пошуку), послідовність і конкретні терміни проведення кожної слідчої дії. Відповідні завдання вирішуються на підставі аналізу матеріалів кримінального провадження [207, с. 87].

Як зазначає Т. А. Абушов, «…проведення обшуку складається з низки організаційних і тактичних заходів, спрямованих на виконання таких

завдань: ознайомлення обшуканого з процесуальними документами, що дають дозвіл на проведення обшуку; процесуальне оформлення залучення учасників обшуку, роз'яснення прав та обов'язків, мети й порядку проведення обшуку, повідомлення про застосування технічних засобів, забезпечення реалізації їх прав та обов'язків; створення умов для постійного та якісного безпосереднього контакту учасників обшуку з об'єктом, який досліджують відповідно до попереднього розподілу завдань (шуканий об'єкт, власник приміщення, члени родини); забезпечення інформаційної взаємодії між учасниками обшуку та досліджуваними об'єктами за допомогою методів пізнання; одержання нової матеріальної доказової та орієнтуючої інформації, визначення її джерел; перевірка, уточнення, доповнення наявної у справі інформації; забезпечення цілісності шуканих об'єктів від дій осіб, зацікавлених у їх не виявленні, фальсифікації або знищенні; усунення протиріч, що мають місце в матеріалах кримінальної справи, яку розслідують; перевірка загальних та окремих криміналістичних версій стосовно розслідування загалом і обставин, що перевіряють під час проведення обшуку, внесення до них відповідних корективів, висунення їх підстав і нових версій; одержання слідчим у процесі обшуку доказової та іншої інформації від учасників обшуку; фіксація перебігу проведення та результатів обшуку» [1, с. 201]

Зокрема, Л. П. Паламарчук акцентує увагу на тому, що матеріальні сліди також можуть залишатися на обчислювальній техніці (сліди від пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо), а також на магнітних носіях і оптичних дисках. На його думку, до окремого типу належать інформаційні сліди, що утворюються внаслідок впливу на комп'ютерну інформацію (шляхом знищення, перекручення). Автор зазначає, що вони залишаються на магнітних носіях інформації і пов'язані зі змінами, які відбулися у самій інформації порівняно з початковим її станом. Також до інформаційних слідів належать наслідки роботи антивірусних і тестових програм, які можуть бути виявлені під час вивчення комп'ютерного

обладнання, робочих записів програмістів, протоколів роботи антивірусних програм та програмного забезпечення. Для виявлення подібних слідів необхідно залучати спеціаліста з комп'ютерної техніки та програмного забезпечення [142, с. 8].

О. Л. Мусієнко акцентує увагу на тому, що обшук у приміщеннях, особливо обшук житла, дуже складний. Необхідно мати уявлення про основні властивості досліджуваних об'єктів, що забезпечить перевірку різних конструктивних порожнин і ділянок, де можуть бути створені сховища (тайники). Методи дослідження житлових приміщень (при обшуку) у справах про шахрайство не мають істотних відмінностей від обшуків за іншими категоріями справ. Обшуку в приміщенні має передувати в ряді випадків вивчення родинних, особистісних та інших зв'язків підозрюваного. Це дозволить здійснити обшуки не тільки за місцем проживання підозрюваного. Автор вказує на те, що іноді шахраї залишають або передають на зберігання предмети й документи своїм знайомим, родичам, іншим особам [121, с. 130].

Підводячи підсумок, необхідно відмітити, що проведення обшуку в кримінальних провадженнях щодо шахрайства, вчиненого у сфері використання банківських електронних платежів, дає можливість підвищити рівень, якість і ефективність розслідування.

Однією з найбільш розповсюджених СРД є огляд. Як зазначає окрема група науковців (В. А. Журавель, В. О. Коновалова, В. Ю. Шепітько), огляд – це слідча дія, яка полягає у безпосередньому сприйнятті об'єктів з метою виявлення слідів злочину та інших речових доказів, з'ясування обставин події, а також обставин, що мають значення у справі [92, с. 161]. Під час проведення огляду, отримані результати як правило є початковим матеріалом, від яких буде залежати подальше розслідування протиправного діяння.

Відповідно до ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення

слідчий, прокурор проводять огляд місцевості, приміщення, речей та документів. Так як питання тактики проведення огляду достатньо висвітлені у криміналістичній літературі, розглянемо їхні особливості при розслідуванні злочинів, кваліфікованих за ст. 190 КК України [96].

Провівши аналіз кримінальних проваджень про шахрайство у сфері банківських електронних платежів, огляд місця події проводиться в 59 %, а ефективність виявляється не більше 40 %, так як здебільшого даний вид протиправного діяння розтягнутий у часі і як правило фактичне місце вчинення важко встановити. Для виявлення фактичного місця шахрайства залучаються відповідні ІТ-фахівці з кібербезпеки.

Доречною вважаємо думку І. В. Пирога, який вказує на те, що підвищення рівня професіоналізації злочинності, витонченості способів учинення та приховування злочинів, укріплення їх технічного оснащення зумовлює необхідність упровадження в практику протидії злочинності сучасних науково-технічних засобів та ефективних методів. Автор наголошує на тому, що зі зміною структури злочинності, її скерованості на нові види кримінальних правопорушень (економічної спрямованості, учинених з використанням вибухових пристроїв, телекомунікаційних та електронних мереж тощо), у тому числі пов’язаних із використанням новітніх науково-технічних засобів, слідчому дедалі складніше провадити розслідування без широкого використання спеціальних знань [144, с. 31]. Підтримуючи вказану позицію, зазначимо, що в розрізі проведення ОМП по досліджуваній категорії кримінальних проваджень залучення спеціаліста має діже важливе значення.

В свою чергу, В. І. Пазиніч виокремлює дві групи типових об’єктів огляду: «…приміщення, автотранспорт та інші місця, де здійснювалося зберігання, клонування мобільних телефонів, виробництво інших радіоелектронних пристроїв, підробка документів; предмети, пов’язані зі вчиненням злочинів у сфері мобільних телекомунікацій: мобільний телефон злочинця, інші радіоелектронні пристрої, засоби комп’ютерної техніки

злочинця і оператора мобільного зв'язку, паперові носії інформації» [141, с. 28].

Така процесуальна дія слугує виявленню, фіксації, та вилучення слідів кримінального правопорушення, а також для обстановки місця події. Сліди протиправного діяння при такому виду шахрайства є не стандартними та знаходяться в електронному вигляді та на електронних носіях. При огляді електронних інформаційних систем (комп'ютер, планшет, мобільний телефон, тощо) об'єктом огляду являється така техніка, а також носії інформації (на приклад IP адреси, системні дані, програми, cookies браузерів, КЕШ та ін.).

До специфіки ОМП при розслідуванні шахрайства в сфері банківських електронних платежів, на наш погляд, слід віднести такі дії: вилучення в ході ОМП з електронних носіїв тої інформації, яка б підтверджувала або навпаки спростовувала факт шахрайства в діях підозрюваних в даному виду протиправного діяння, зразків друку принтерів або самих принтерів (для виготовлення підроблених документів, банківських карток тощо), виявлення спец засобів для перехоплення та зчитування даних та ін.

Зі свого боку, О. В. Курман вказує на важливу роль в розслідуванні шахрайства з фінансовими ресурсами відіграє слідчий огляд документів [106, с. 11]. Тобто при розслідуванні шахрайства мають значення своєчасне та тактично правильне вилучення документів. Аналіз відповідного способу вчинення шахрайства, урахування місця та засобів вчинення, також використання документів на предмет посягання протиправного діяння дозволяють уповноваженій особі визначити вид та перелік документів які підлягають вилученню.

Документи які можуть бути предметом вилучення можуть знаходитись не лише за місцем вчинення шахрайства, але й в інших установах, організаціях, підприємствах. В такому випадку уповноваженій особі треба визначити точне місце перебування таких документів. Прикладом може слугувати виписка по рахункам, документи підтверджуючі перерахунок коштів, які знаходяться у відповідній фінансовій установі. Після вилучення даних документів проводиться ретельне дослідження.

В свою чергу, І. В. Пиріг наголошує на тому, що спеціаліст, залучений до проведення СРД, володіє необхідними спеціальними знаннями та, користуючись ними, надає допомогу слідчому. При наданні криміналістичної допомоги, що полягає у виявленні, фіксації та вилученні об'єктів, що мають значення для розслідування, та технічної (використання пошукових приладів, сприяння огляду у важкодоступних місцях із залученням спеціального обладнання тощо) спеціаліст обов'язково пояснює слідчому та іншим учасникам, у тому числі понятим, які дії він виконує, які пристрої застосовує, наслідки та результати використання спеціальних знань, вмінь та навичок. Автор вказує, що матеріальні об'єкти, виявлені та вилучені під час проведення СРД, описуються у протоколі та належним чином упаковуються. Відомості про технічні засоби, що використовувалися під час проведення СРД, та результати їх застосування також містяться у протоколах або додатках до них. Однак результати дослідницьких дій на місці події, що проводяться як самим слідчим, так і залученим до огляду спеціалістом та становлять основу для висунення слідчих версій, не завжди фіксуються у протоколі. Криміналістичні рекомендації щодо складання протоколу огляду забороняють заносити у протокол будь-які думки, коментарі або пояснення їх учасників [143, с. 222].

Підводячи підсумки, зазначимо, що при ОМП при розслідуванні шахрайства в сфері банківських електронних платежів треба враховувати специфіку об'єктів, які оглядаються. При огляді треба залучати відповідних ІТ-фахівці з кібербезпеки з залученням спеціальних технічних засобів для виявлення, встановлення та вилучення певної інформації, яка знаходиться на електронних носіях та слугуватиме доказами по даному кримінальному правопорушенню. Адже місце події для уповноваженої особи носить дослідницький характер, спрямований на встановлення обстановки події, виявлення слідів протиправного діяння та з'ясування інших обставин, які можуть пришвидшити його розкриття [68, с. 125].

3.2. Організаційно-тактичні аспекти проведення негласних слідчих (розшукових) дій

Вчинення шахрайства в сфері використання банківських електронних платежів передбачає вкрай педантичну підготовку шахраїв до вчинення вказаного діяння. З огляду на те, що більшість досліджуваних правопорушень мають «безконтактну» форму (тобто немає візуального контакту між шахраєм та потерпілим) виникає потреба у проведенні ряду НСРД та оперативно-технічних заходів. Адже лише з огляду на їх проведення вбачається можливих документування та доказування вказаних діянь.

Для початку відмітимо, що, як зазначає А. А. Венедіктов, «…формально-юридичний підхід дозволяє одночасно віднести оперативне впровадження (виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації) до різних категорій, що належать до окремих, хоча і взаємопов’язаних державно-правових діяльних систем – ОРД та кримінального процесу. Тому, залишаючись незмінним за своїм змістом, оперативне впровадження як засіб пізнавальної діяльності правоохоронних органів може мати дві різні юридичні форми залежно від сфери застосування. Це зумовлює потребу з’ясування взаємозв’язку та відособленості виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації як ОРЗ та як НСРД» [24, с. 74].

Згідно положень Інструкції «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» та ст. 246 КПК України, негласні слідчі (розшукові) дії – це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених КПК [97; 149]. Тобто є специфічні методи проведення вказаних процесуальних дій.

В свою чергу, В. А. Колесник зазначає, що утаємниченими такі відомості мають бути не лише від осіб, стосовно яких проводяться ці негласні дії, а й від будь-яких інших осіб, зокрема й працівників органів досудового розслідування, оперативних підрозділів, посадових осіб правоохоронних та інших органів, пересічних громадян тощо, які не задіяні в підготовці й проведенні конкретних негласних слідчих (розшукових) дій, навіть якщо вони беруть участь в інших заходах із здійснення досудового розслідування у конкретному кримінальному провадженні. Автор відмічає, що саме негласність виступає тим чинником, який істотно впливає на визначення видів НСРД, отримання відповідних дозволів та встановлення порядку їх проведення, визначення основних виконавців і кола учасників, обрання способу фіксування перебігу й результатів проведення. Вчений акцентує увагу на тому, що особливі процесуальні вимоги впливають і на розроблення специфічних тактичних прийомів і тактико-криміналістичних рекомендацій з проведення НСРД та використання їх результатів у доказуванні [78, с. 130]. Тобто необхідність максимально таємного проведення вказаних процесуальних дій викликає потребу в наявності відповідних наказів з грифом «Таємно» або «Цілком таємно».

В той же час, Глава 21 КПК присвячена висвітленню повного списку можливих НСРД: 1) аудіо-, відеоконтроль особи (ст. 260 КПК); 2) накладення арешту на кореспонденцію (ст. 261 КПК); 3) огляд і виїмка кореспонденції (ст. 262 КПК); 4) зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК); 5) зняття інформації з електронних інформаційних систем (ст. 264 КПК); 6) обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК); 7) встановлення місцезнаходження радіоелектронного засобу (ст. 268 КПК); 8) спостереження за особою, річчю або місцем (ст. 269 КПК); 9) аудіо-, відеоконтроль місця (ст. 270 КПК); 10) контроль за вчиненням злочину, формами якого є контрольована поставка, контрольована та оперативна закупка, спеціальний слідчий експеримент, імітування обстановки злочину (ст. 271 КПК); 11) виконання

спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК); 12) негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК) [97].

Як доречно вказує група авторів (М. А. Погорецький, Д. Б. Сергєєва), що не підлягає розголошенню також і факт проведення НСРД. Вчені зазначають, що постанова слідчого, прокурора про проведення НСРД, клопотання про дозвіл на проведення НСРД, ухвала слідчого судді про дозвіл на проведення НСРД та додатки до нього, протокол про проведення НСРД підлягають засекречуванню в порядку, встановленому законодавством [146, с. 138]. Ми однозначно підтримуємо зазначену позицію, адже зрозуміло, що вказані умови максимально забезпечать ефективність проведення досліджуваних процесуальних дій.

Досить доречно А. Слободзян відмічає, що суб'єкти НСРД під час виконання завдань, визначених актами законодавства, виконують кримінально-процесуальні функції, які забезпечують: «…додержання конституційних прав та законних інтересів учасників досудового розслідування, інших осіб; швидке, повне та неупереджене розслідування злочинів; дотримання режиму секретності; захист особи, суспільства і держави шляхом встановлення істини, викриття винної особи, із застосуванням організаційних, практичних прийомів, у тому числі технічних засобів, що дають змогу в порядку, передбаченому кримінальним процесуальним законодавством України, отримати інформацію про злочин або особу, яка його вчинила, без її відома» [179, с. 89-90]. Ми повністю підтримуємо думку авторки, оскільки лише виконання вказаних функцій забезпечить ефективне виконання НСРД в провадженням будь-якої категорії.

В свою чергу, С. В. Самойлов аргументував доцільність використання такого способу отримання доказової інформації під час досудового розслідування, як витребування інформації від установ та організацій. Автор визначив, що його ефективність прямо залежить від того, наскільки слідчий тактично грамотно зробить відповідний запит, чому сприяє дотримання

наступних умов: а) своєчасності запиту; б) законності запиту; в) визначення вичерпного переліку інформації, яку необхідно з'ясувати шляхом запиту. Вчений надав перелік адресантів та перелік інформації, яку можливо таким чином отримати, а також запропонував конкретну форму запиту [168].

Доречною вважаємо позицію В. А. Колесника, який зазначає, що запровадження НСРД, що здійснюються слідчим або уповноваженими оперативними підрозділами під час досудового розслідування, не скасовує права оперативно-розшукових підрозділів на здійснення у гласній та негласній формі оперативно-розшукової діяльності, вагома частка результатів якої має значення для встановлення фактичних обставин вчинення злочину і тому використовується в кримінальному провадженні. Автор наголошує на тому, що завдання й способи проведення багатьох НСРД зумовлюють потребу використання їх суб'єктами допомоги співробітників відповідних оперативних підрозділів і застосування спеціальних технічних засобів виявлення й фіксації інформації, що зазвичай використовуються в практиці роботи оперативно-розшукових підрозділів. Вчений робить висновок, що порядок, режим, тактичні прийоми використання в доказуванні результатів НСРД та результатів негласних оперативно-розшукових заходів, навіть назви яких є іноді подібними, істотно відрізняються. Це зумовлено різною природою походження й різним порядком та суб'єктами отримання таких матеріалів [77, с. 6-7].

Зі свого боку, окрема група авторів (Л. М. Грібов, С. М. Пугач) наголошують, що при проведенні НСРД у публічно доступних місцях дозволено вільно використовувати технічні засоби аудіо- і відеоконтролю, фотографування, відео- та звукозапису; технічні засоби встановлення місця знаходження конкретних матеріальних об'єктів; оптичні прилади, технічні засоби зв'язку, транспортні засоби. Вчені відмічають, що місцем проведення НСРД є місце знаходження осіб, що беруть у ній участь, і технічних засобів, що ними використовуються. Крім того, науковці роблять висновок, що уповноважені оперативні підрозділи, виконуючи доручення слідчого,

прокурора, можуть використовувати наявні у них засоби, якщо вони відповідають вимогам цього Кодексу щодо засобів, які використовуються при проведенні НСРД [33, с. 5]. Як бачимо, в деяких випадках можна проводити НСРД в місцях вільного доступу без обов'язкових процесуальних обмежень.

А вже Д. В. Безруков акцентує увагу на тому, що необхідно розглянути питання забезпечення прав людини та внутрішньої безпеки держави в умовах використання оперативно-технічних заходів та НСРД підрозділами карного розшуку питання. Автор зазначає, що «…досвід останніх десятиліть свідчить про те, що такі інститути як права людини і суспільна безпека не тільки є двома самостійними пріоритетними напрямками діяльності держави, але і дуже тісно пов'язані один з одним. Наприклад, аксіоматичним є положення – незабезпечення безпеки суспільства неминуче приводить до порушення багатьох прав людини. Разом з тим існує і зворотний зв'язок: якщо якісь права людини надмірно розширені, то знижується ефективність правоохоронної діяльності, отже, знижується рівень безпеки суспільства» [14, с. 170].

Стосовно процесу документування, то ми підтримуємо позицію групи науковців (О. М. Джужа, Є. М. Моісеєв, Д. Й. Никифорчук), які розділили вказаний процес на дві групи: «1. Виявлення фактичних даних. 2. Забезпечення можливості їх використання при розслідуванні. Для першого елементу характерне отримання інформації та її перевірка. Автори вказують, що «виявлення фактичних даних – це сукупність оперативно-розшукових дій, які забезпечують отримання відомостей, що підтверджують злочинні діяння розроблюваних осіб. Це такі фактичні дані: про подію злочину (час, місце, спосіб); про причетність розроблюваного до підготовки або вчинення злочину; про обставини, які сприяли вчиненню злочину; коло осіб, причетних до його вчинення; місцезнаходження документів, предметів, цінностей, отриманих злочинним шляхом; обставини, що характеризують особу, пом'якшуючі, обтяжуючі обставини» [130, с. 238].

В свою чергу, О. В. Пчеліна формулює наступний перелік допустимих заходів гласного та негласного характеру при розслідуванні службових кримінальних правопорушень: «…оперативна перевірка підозрюваного на причетність до вчинення інших злочинів, у тому числі у сфері службової діяльності; здійснення перевірки за інтегрованими ІПС Національної поліції України, єдиними та державними реєстрами, іншими пошуковими системами в електронних мережах загального користування з метою отримання довідково-аналітичної та оперативно-пошукової інформації, у тому числі про аналогічні нерозкриті злочини; отримання консультаційної допомоги від фахівців; вилучення документації, пов'язаної зі службовою діяльністю підозрюваного, шляхом проведення відповідних обшуків, тимчасового вилучення чи отримання тимчасового доступу до неї; огляд вилученої документації, аналіз її змісту та виявлення слідів імовірної фальсифікації; призначення технічних і почеркознавчих експертиз документів; проведення ревізій, зустрічних та інших перевірок; огляд приміщень, земельних ділянок, споруд, устаткування тощо; отримання зразків для експертизи, за необхідності негласне отримання зразків, необхідних для порівняльного дослідження; призначення судово-економічної, будівельно-технічних та інших судових експертиз; допит підозрюваного та свідків; здійснення аудіо-, відеоконтролю особи злочинця та місця; зняття інформації з транспортних телекомунікаційних мереж, отримання розшифрування телефонних розмов і проведення їх аналізу; зняття інформації з інформаційних систем» [155, с. 291].

Як зазначає О. В. Курман, шахрайство з фінансовими ресурсами відноситься до таких кримінальних правопорушень, які в більшості випадків виявляються оперативним шляхом (86,4 %). Автор наголошує на тому, що планування розслідування за справами, внесеними на основі оперативно-розшукових матеріалів, є специфічним. Одна із особливостей планування досудового розслідування за справами цієї категорії – забезпечення зашифровування шляхів одержання даних про осіб, які здійснили

протиправне діяння, необхідність поєднання СРД з оперативно-розшуковими заходами в процесі всього розслідування, а також забезпечення можливості легалізації інформації, одержаної оперативним шляхом [105, с. 217].

Зі свого боку, Д. А. Нескоромний акцентує увагу на тому, що «…провадження НСРД при розслідуванні кримінальних правопорушень, вчинених ОЗГ, крім отримання доказів, дозволяє отримати дані щодо конкретної організованої злочинної групи, здійснювати аналіз отриманої інформації щодо чисельності ОЗГ, її складу, структури, зв'язків між членами ОЗГ, їх пособниками, наявність у них корупційних зв'язків. НСРД являються ефективним способом отримання відомостей, речей і документів, які мають значення для досудового розслідування» [125, с. 23]. Тобто для досліджуваної категорії кримінальних проваджень застосування вказаних процесуальних дій однозначно має велике значення.

В свою чергу, А. Гетьман акцентує увагу на тому, що візуальне спостереження може здійснюватися з метою негласного спостереження, слідкування за особами, підозрюваними у вчиненні тяжких або особливо тяжких злочинів (об'єктів спостереження), місцями їх постійного проживання чи тимчасового перебування, за їх поведінкою, транспортними засобами, які вони використовують. Автор зазначає, що візуальне спостереження повинна бути спрямована на отримання об'єктивної інформації про протиправну діяльність окремих осіб, їх співучасників, виявлення зв'язків цих осіб, встановлення місцезнаходження осіб, які розшукуються органами досудового розслідування чи судом, з'ясування обставин безвісного зникнення людей, а також встановлення місць зберігання знарядь, предметів учинення злочинів і незаконно добутого майна. Вчений як підсумок зазначає, що візуальне спостереження за конкретною особою завжди має на меті пошук і фіксацію відомостей, що можуть використовуватись у доказуванні, а також з метою забезпечення інших слідчих і процесуальних дій: установлення місцезнаходження радіоелектронного засобу, контрольованих та оперативних закупок товарів,

затримання підозрюваного тощо [27]. Як бачимо, все перераховане підходить до процесу розслідування шахрайства в сфері використання банківських електронних платежів.

А вже В. Д. Безруков розділяє НСРД за характером дії суб'єктів кримінального провадження стосовно отримання даних з телекомунікаційних мереж, а саме: «…1) зняття інформації з транспортних телекомунікаційних мереж (НСРД, передбачена ст. 263 КПК України), що в свою чергу поділяється на: конспіративне перехоплення, контроль телефонних розмов та фіксацію їх змісту з використанням технічних засобів негласного отримання інформації; перехоплення електронних сигналів та повідомлень з використанням технічних засобів негласного отримання інформації; 2) установлення місцезнаходження радіоелектронного засобу шляхом: пеленгування місцезнаходження кінцевого обладнання мереж телекомунікацій оперативно-технічними підрозділами при виконанні доручень у порядку ст. 40 КПК України – як НСРД «установлення місцезнаходження радіоелектронного засобу», передбачена ст. 268 КПК України; затребування компетентними органами розслідування інформації про взаємоз'єднання телекомунікаційних мереж з метою отримання та вибірки відомостей про надані телекомунікаційні послуги – як процесуальна дія, передбачена ст. 93 КПК України» [13, с. 172].

Доречною є позиція групи науковців (С. С. Кудінов, Р. М. Шехавцов., О. М. Дроздов, С. О. Гриценко), які акцентують увагу на тому, що підставами, достатніми для втручання у приватне спілкування, є: «…фактичні дані, отримані у передбаченому КПК порядку, що розмови особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування, поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб, певна електронна інформаційна система можуть містити відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування; можливість отримання відомостей про зміст

приватного спілкування тільки шляхом проведення НСРД, що включають втручання у приватне спілкування» [100, с. 36]. В розрізі зазначеного відмітимо, що при розслідуванні шахрайства в сфері використання банківських електронних платежів обов'язково повинна бути наявна можливість для втручання у приватне спілкування шахраїв.

Зі свого боку, О. В. Керевич відмічає, що при реалізації НСРД уповноважені оперативні підрозділи не мають права виходити за межі доручень слідчого, прокурора. Автор наголошує на тому, що вони зобов'язані повідомляти їх про виявлення обставин, які мають значення для кримінального провадження або вимагають нових процесуальних рішень слідчого, прокурора. Далі ситуація відбувається у доволі забюрократизованій формі. Так, відповідно до «Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні», отриману інформацію в ході проведення встановлення місцезнаходження радіоелектронного пристрою та (або) спостереження за особою річчю або місцем, оперативні підрозділи, які залучалися, передають підрозділам ініціаторам для складання протоколу. Далі, після складання, протокол і додатки до нього, не пізніше 24 годин після складання, надаються прокурору, зазначеному в дорученні. Після чого прокурор, за необхідності, може ознайомити слідчого, який здійснює розслідування даного кримінального провадження з протоколом і відповідними додатками. Потім відбувається процес розсекречення протоколу й додатків проведення відповідних НСРД та додавання їх до матеріалів кримінального провадження [61, с. 104].

На основі вивчення матеріалів кримінальних проваджень, нами було встановлено, що специфічною ознакою шахрайства в сфері використання банківських електронних платежів є потреба проведення цілого ряду НСРД та оперативно-технічних заходів, пов'язаних із встановленням шахрая та його зв'язків. Зокрема, серед них необхідно виокремити такі як спостереження за об'єктом або особою; огляд кореспонденції; прослуховування телефонних переговорів; зняття інформації з транспортних та електронних систем.

На основі аналізу матеріалів кримінальних проваджень [Додаток А], нами було виявлено наступні труднощі, що виходять з реалізації відомостей НСРД при розслідуванні шахрайства в сфері банківських електронних платежів, наприклад:

– незлагоджена взаємодія підрозділів правоохоронних органів та працівників установ зв'язку (69 %);

– проблематичність одержання ухвали слідчого судді апеляційного суду стосовно проведення певної НСРД (61 %);

– відсутність бажання окремих уповноважених осіб покращувати процес кримінального провадження, а також потяг до пошуку більш легких шляхів для отримання доказової інформації (32 %);

– брак потреби в огляді та вилученні документів (48 %).

Стосовно результатів НСРД, ми повністю поділяємо позицію Д. Б. Сергєєвої, яка зазначає, що вони розглядаються лише як матеріально фіксовані джерела, що виникають в процесі проведення негласних слідчих (розшукових) дій та містять певну інформацію, відомості, тобто у вузькому значенні цього терміну. Авторка вказує на те, що результати НСРД для їх подальшого використання, в тому числі й у кримінальному процесуальному доказуванні, мають бути трансформовані в передбачену матеріальну форму – відповідні матеріали НСРД. Вчена робить висновок, що сама лише змістовна складова результатів їх проведення – інформація, що отримується в результаті їх проведення, не дозволяє її використовувати в інтересах кримінального судочинства [176, 102].

Констатуючи вищезазначене, необхідно вказати, що реалізація НСРД відповідно до процесуального порядку є неодмінною умовою того, щоб їх результати здійснення суд вбачав допустимими. Також вважаємо доречним наголосити на тому, що важливим є вилучення в установі зв'язку під час огляду затриманої кореспонденції, речей та документів, які мають значення для певного кримінального провадження.

3.3. Особливості призначення експертиз у кримінальних провадженнях досліджуваної категорії

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. Незважаючи на масу переваг, ця ситуація активізувала спалах вчинення кримінальних правопорушень, кількість яких збільшуються щорічно, зокрема, шахрайство в сфері банківських електронних платежів. Такі кримінальні правопорушення, як правило, кваліфікуються за ч. 3 ст. 190 КК України [96], а під час їх розслідування призначається судова комп'ютерно-технічна експертиза.

Тому з метою визначення особливостей призначення експертиз як обов'язкових слідчих (розшукових) дій під час розслідування шахрайства у сфері використання банківських електронних платежів, а також дослідження окремих заходів щодо її підготовки, розглянемо низку думок вчених, які досліджували проблематику даного питання.

Із приводу експертиз, що необхідно проводити під час розслідування шахрайства існують різні думки. Для прикладу, Г. С. Бідняк зауважує, що на законодавчому рівні не передбачено визначення поняття спеціальних знань і їхніх форм, та виокремлює такі їх ознаки: «…1) є комплексом знань і навичок у різних галузях; 2) складаються з системи відомостей в галузі

науки, техніки та інших сфер людської діяльності; 3) використовуються в досудовому розслідуванні та судовому провадженні у випадках і в порядку, визначених кримінальним процесуальним законодавством; 4) їх використання здійснюється у взаємозв'язку з науково-технічними засобами; 5) реалізуються визначеним суб'єктом кримінального судочинства у процесі практичної діяльності, спеціальної підготовки з урахуванням професійного досвіду і засновані на системі теоретичних знань у відповідній галузі; 6) їх реалізація вимагає значних витрат часу й інтелектуальних зусиль; 7) сприяють у розробці технічних засобів і прийомів роботи з доказами та встановленню вагомих обставин, що мають значення для доказування» [15, с. 41-44].

Наразі, Т. В. Охрімчук акцентувала увагу на тому, що особливу увагу слід звернути на проведення судових експертиз. Авторка вказану позицію аргументувала тим, що під час розслідування шахрайства з фінансовими ресурсами виникає потреба у проведенні судово-економічної, судово-бухгалтерської експертизи та судової фінансово-кредитної експертизи. Крім того, вчена зазначала, що може виникнути потреба у проведенні криміналістичних експертиз: технічної експертизи документів, почеркознавчої, авторознавчої тощо [135, с. 62].

Інші автори (О. В. Одерій, С. В. Самойлов) вказували, що з огляду на специфічність та різноплановість способів вчинення шахрайств із використанням мережі «Інтернет», слід орієнтує нотуватися на призначення конкретних судових експертиз і визначати коло питань, які можуть бути поставлені перед експертами [172, с. 109].

Зі свого боку, Т. В. Коршикова на основі вивчення результатів кримінальних проваджень щодо шахрайств, які вчиняються з використанням ЕОТ, визначила «…наступні види експертизи, які призначались при їх розслідуванні, зокрема щодо вилучених: електронно-обчислювальна техніка (комп'ютерно-технічна експертиза (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення),

дактилоскопічна експертиза вилучених слідів рук з різних предметів ЕОТ); телекомунікаційні засоби та системи (експертиза телекомунікаційних систем і засобів); документи (експертиза документів, які утворювались внаслідок вчинення шахрайських дій – криміналістична почеркознавча експертиза; технічна експертиза документів; дактилоскопічна експертиза вилучених слідів рук з документів); майно, яке було предметом посягання (криміналістична експертиза матеріалів, речовин і виробів; трасологічна експертиза; дактилоскопічна експертиза вилучених слідів рук з різних предметів)» [89, с. 297].

О. Л. Мусієнко наголошує на тому, що останнім часом шахраї все частіше для вчинення злочинного посягання використовують комп'ютерну техніку, електронні пристрої (при шахрайстві на ігрових атракціонах). Автор робить висновок, про необхідність призначення достатньо нових видів експертиз: комп'ютерно-технічної експертизи, комп'ютерно-мережевої експертизи. Науковець зазначає, що КТЕ залежно від завдань, що вирішуються, поділяється на два різновиди: 1) технічна експертиза комп'ютерів, їх вузлів та пристроїв (встановлення призначення і характеристик комп'ютерної техніки, її технічного стану; можливостей використання для досягнення певної мети тощо); 2) експертизи даних та програмного забезпечення (виявлення інформації, що міститься на комп'ютерних носіях, та визначення її цільового призначення; відновлення знищеної інформації; встановлення характеру змін, внесених у програми тощо). На думку О. Л. Мусієнка, вказана експертиза дозволяє вирішувати такі питання: «…1) чи справний даний пристрій (ігровий комп'ютер, електронна рулетка тощо); 2) чи має даний пристрій дефекти, якщо так, то які саме; 3) чи не мають поломки вузли цього пристрою; 4) чи відповідає це обладнання технічній документації; 5) чи правильно встановлено програмне забезпечення цього пристрою; 6) чи можливо змінити програмне забезпечення цього пристрою, якщо так, то яким способом; 7) чи можливо керувати пристроєм на відстані, якщо так, то на якій відстані і яким чином;

8) чи можлива нормальна експлуатація пристрою після внесення змін в програмне забезпечення; 9) як забезпечується та чи надійна система захисту інформації від доступу; 10) чи можливо на даному комп'ютері використати програму в обхід автоматичної її реєстрації» [121, с. 134].

Цікавою є думка С. С. Чернявського, який зазначає, що узагальнення вітчизняного і зарубіжного досвіду призначення та проведення судово-бухгалтерської, фінансово-економічної почеркознавчої експертиз, техніко-криміналістичної експертизи документів, комп'ютерно-технічних експертиз є необхідною передумовою подальшого удосконалення окремих методик розслідування фінансового шахрайства [205, с. 19]. І дійсно, для удосконалення методики розслідування шахрайства в сфері використання банківських електронних платежів необхідно розглянути питання призначення окремих видів експертиз.

Одною з основних процесуальних дій при розслідуванні шахрайства в сфері банківських електронних платежів є призначення судової комп'ютерно-технічної експертизи.

СКТЕ призначається у випадках, коли необхідно отримати фактичні дані для розслідування кіберзлочинів із використанням електронно-обчислюваної техніки, якими являються факти вчинення шахрайства в сфері банківських електронних платежів, для створення доказової бази в кримінальних провадженнях.

КТЕ – це підвид інженерно-технічної експертизи [55], за якої досліджуються певні технічні характеристики обчислювальної техніки, а саме стаціонарних комп'ютерів (ПК), смартфонів, ноутбуків, планшетів, нетбуків тощо, та проводиться детальний аналіз програм, установлених на даних технічних засобах, із метою виявлення інформації, що знаходиться в електронному вигляді на даних пристроях, для встановлення факту скоєння кримінального правопорушення. За допомогою експертизи виявляються ознаки кримінального правопорушення, що слугують створенню доказової бази шляхом аналізу виявленої інформації [41].

Як зазначають експерти, до основних завдань експертизи комп'ютерної техніки і програмних продуктів належать: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку [82].

Із цього приводу, О. А. Самойленко доречно вказує, що аналіз спеціальної літератури й нормативних джерел дав можливість визначити, що КТЕ – це дослідження технічних властивостей комп'ютерного (цифрового) обладнання, програмного забезпечення, інформації, що містяться на цифрових носіях, із метою встановлення фактичних даних, які мають значення для провадження та пов'язані із застосуванням комп'ютерної техніки, а також виявляються на підставі спеціальних знань у галузях комп'ютерної техніки та програмування. Авторка зазначає, що об'єктами судової експертизи є комп'ютери з носіями інформації (будь-які накопичувачі інформації – дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (наприклад, мобільні телефони, банкомати, гральні автомати, картридери, електронні записні книжки, пейджери, принтери тощо), а також документація до обладнання [164]. Тобто ефективність розслідування кримінальних правопорушень, таких як шахрайство в сфері банківських електронних платежів, залежить від своєчасного виявлення слідів кримінального правопорушення, адже у випадку, якщо СРД будуть проведені невчасно та із запізненням, зловмисники можуть знищити всю доказову базу, а саме виконати форматування жорсткого диску, фізичне знищення жорсткого диску за допомогою мікрохвильової печі, USB-накопичувачів, зовнішніх накопичувачів, CD-, DVD-дисків тощо.

Для того щоб сліди, що знаходяться на електронних носіях, стали доказами, їх слід знайти, виявити та зафіксувати процесуальним шляхом,

що регулюється ЗУ «Про судову експертизу» [153].

Факти та обставини, що виявляються в процесі аналізу апаратно-технічних засобів та програмного забезпечення, встановленого на цих засобах, які є доказами у матеріалах кримінального провадження, є предметом СКТЕ [40, с. 118-119].

Експерти з ННЦ «Інститут судових експертиз імені Заслуженого проф. М. С. Бокаріуса» визначили наступний орієнтовний перелік вирішуваних питань для КТЕ: «…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?» [82].

Залежно від обставин кримінального провадження можуть бути призначені такі види експертиз:

– апаратно-комп'ютерна експертиза (АКЕ);

– програмно-комп’ютерна експертиза (ПКЕ);

– комп’ютерно-мережева експертиза (КМЕ);

– інформаційно-комп’ютерна експертиза(ІКЕ).

Об’єктом дослідження апаратно-комп’ютерної експертизи (далі по тексту – АКЕ) може бути саме техніка, за допомогою якої вчинялось шахрайство в сфері банківських електронних платежів. До апаратних засобів відносяться: електричні, електронні та механічні схеми, блоки, прилади і пристрої, що становлять матеріальну частину комп’ютерної системи. При проведенні даної експертизи досліджуються ноутбуки, системні блоки, по яких встановлюється вид та назва процесора (CPU), вид та назва материнської плати (motherboard), вид оперативної пам’яті (RAM), назва відеокарти (GPU), вид жорсткого накопичувача(HDD або SSD). Встановлення видів і назв технічних засобів дозволяє порівняти їх із слідами, залишеними злочинцем на серверах банківських установ або організацій, що піддалися шахрайським діям. Головним ідентифікаційним фактором комп’ютера, із якого проводились шахрайські дії, є так званий ідентифікаційний номер ПК (MAC-адреса). MAC-адреса (Media Access Control, адреса управління доступом до середовища) записується до заводської прошивки мережевого адаптера при його виготовленні [217]. Він потрібен для того, щоб ідентифікувати конкретний мережевий адаптер, який знаходиться на материнській платі. Кожен пакет даних, що приймається адаптером, містить його MAC-адресу, для того щоб пристрій міг зрозуміти, що ці дані призначені саме йому. MAC-адреса ПК подібна відбиткам пальців, якщо злочинець при вчиненні шахрайських операцій у сфері банківських електронних платежів, був необережний в своїх діях та не замінив MAC-адресу за допомогою спеціальних програм, то його обчислювана техніка, за допомогою якої шахрай вчиняв суспільно небезпечне діяння, буде ідентифікована.

При проведенні АКЕ експерту необхідно зупинитися на таких моментах:

– виявити відношення досліджуваної техніки до апаратних комп’ютерних засобів;

– визначити тип, марку або модель даного пристрою;

– встановити технічні характеристики і параметри досліджуваного технічного засобу;

– визначити первинну конфігурацію і характеристики даного пристрою, а також дізнатись, чи були змінені його функціональні властивості, у порівнянні з первісною конфігурацією;

– провести зовнішній огляд техніки на предмет фізичного втручання у його конфігурацію;

– встановити, чи є даний технічний засіб накопичувачем інформації, та чи відкритий доступ до такої інформації.

Дослідження саме програмного забезпечення, встановленого на техніці потенційного зловмисника, являє собою ПКЕ.

Предметом ПКЕ є закономірності розробки програмного забезпечення на електронно-обчислювальній техніці, що була передана для дослідження та виявлення слідів кримінального правопорушення, а також закономірності його застосування.

Завданням ПКЕ є встановлення наявності певних видів програм, що сприяють вчиненню шахрайських операцій у сфері банківських електронних платежів. Ними можуть бути програми, призначені для віддаленого доступу до інформації та керування комп’ютером, наприклад: AnyDesk, Supremo Remote Desktop, TeamViewer, RemotePC тощо. Важливою являється наявність програм, призначених для анонімного та зашифрованого спілкування в мережі Інтернет, таких як Jabber, Telegram, WhatsApp та ін. Як правило, зловмисники можуть використовувати графічні редактори для підробки документів, наприклад Adobe Photoshop, Corel Draw, тощо, тому експерт повинен ідентифікувати їх наявність та встановити історію застосування таких додатків, відновити файли, створені за допомогою цих програм, і, таким чином, виявити важливі сліди вчинення

злочину, що можуть стати важливими доказами в кримінальному провадженні. Не менш вагомою знахідкою можуть бути програми для віддаленого керування банківськими рахунками – інтернет-банкінг, які зловмисники зазвичай використовують на смартфонах та планшетах. За виявлення вищезазначеного програмного забезпечення експерту потрібно встановити або відновити log-файли використання цих програм, що дозволить виявити ланцюг операцій та послідовність дій шахрая.

ІКЕ, як ключовий вид СКТЕ, може стати одним з основних доказів, які можуть вказувати на причетність (або непричетність) до кримінального правопорушення і стати підставою при визначенні вини. Завданням ІКЕ є виявлення наявних або видалених файлів, на яких може міститися значуща для слідства інформація. Особливу увагу експерт має приділити файлам документів формату .doc, .docx, .txt, .rtf, .pdf, .xls, .xlsx та ін., log-файлам електронної пошти та месенджерів.

Під час виконання ІКЕ, також необхідно з'ясувати, чи встановлено на техніці, що була представлена на СТКЕ, програмне забезпечення для шифрування та захисту інформації, що підтверджувала би чи спростовувала здійснення шахрайства в сфері банківських електронних платежів. Шифрування диска створює зашифровані розділи на жорстких дисках або створює віртуальні зашифровані диски у файлі [219, с. 6]. Опісля зашифрування, дані, що зберігаються в розділі, потребують доступу через ведення паролю. Зазвичай, шахраї накладають одразу декілька різних паролів для унеможливлення доступу сторонніх осіб до інформації, яка може викрити їх зловмисні дії. Кожен із таких паролів захищено за допомогою алгоритму шифрування AES 128- або 256-бітного ключа, який дуже важко і практично неможливо розшифрувати, зважаючи на щосекундний розвиток технологій і відсталість в обізнаності новітніх комп'ютерних систем та їх використання в сучасній криміналістиці. Найбільш розповсюдженими програмами шифрування даних є: Folder Lock, AxCrypt, CryptoExpert, CertainSafe, VeraCrypt, TrueCrypt, Bitlocker, Ciphershed.

КМЕ, як один з видів КТКЕ, багато в чому схожий з ПКЕ, однак в даному випадку фокус експертної уваги зміщений на дослідження мережевої роботи користувача. Таким чином вивчаються дії потенційного правопорушника у сфері банківських електронних платежів із залученням комп'ютерних мереж. Для виконання КТЕ фахівець повинен бути компетентним в області мережевих технологій, щоб ефективно відстежувати рух інформаційних пакетів за допомогою вивчення інформаційного сліду.

IP-адреса – це числова послідовність, що слугує ідентифікатором девайсу для Інтернет-сервера [21, с. 5]. IP-адреса відображається у вигляді серії з чотирьох груп чисел, розділених крапками. Перша група – це число від 1 до 255, а інші групи – число від 0 до 255, наприклад 192.135.174.1. Кожен сервер має свою унікальну адресу, за допомогою якої експерти можуть визначити фізичну адресу місця, де було скоєне кримінальне правопорушення. Саме з цієї причини, шахраї намагаються замаскувати такі сліди, використовуючи ряд мережевого програмного забезпечення.

Існують такі розповсюджені способи підміни реальної IP-адреси: підключення до проксі-серверу, використання Інтернет браузера TOR, маскування IP-адреси через VPN.

Під час КМЕ надзвичайно важливо виявити програмне забезпечення, що було встановлене для приховування IP-адреси. Прикладами вищевказаного можуть бути:

– ProxyCap, Proxyfier, Proxy Switcher – програми для проксі;

– TOR Browser, Tor Control (anonymity layer) for Firefox;

– NordVPN, OpenVPN, ExpressVPN, PureVPN for Teams, ProtonVPN, NetMotion – програми, які забезпечують сервіс VPN.

Якщо експертом буде проведено якісне дослідження мережевих слідів та викрито усі ланцюжки IP-адрес, через які проходили транзакції, з великою вірогідністю таке кримінальне правопорушення буде розкрито.

Важливою проблемою в аспекті проведення СКТЕ є її науково-

методичне забезпечення. Відповідно до ст. 85 Конституції України [85], Верховною Радою України було обрано стратегічний курс держави на набуття повноправного членства України в Європейському Союзі, тим самим піднявши високу планку щодо прав та свобод людини, і, як наслідок, збільшивши державну відповідальність перед міжнародними партнерами. Кожній людині гарантовано дотримання принципів при здійсненні правосуддя та проведення експертизи, тобто будуть застосовані одні і ті ж самі методики досліджень незалежно від того, якої форми власності установа, яка проводить експертизу, або який експерт буде її проводити.

Як влучно зазначила І. В. Гора, експертна практика судово-експертними установами повинна буди єдиною як в підходах, так і в роз'ясненнях експертів. Науково-апробовані методики та наукові критерії повинні застосовуватись єдиними стандартами [32, с. 273].

Зокрема, експерти зазначають, 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). Автори вказують, що «…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. З метою дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них. Із 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» [82].

Застосування судовими експертами наукової або спеціалізованої

мови, посилаючись на авторські методики, наукові підходи, у зв’язку з відсутністю у суддів спеціальних знать, сприяє психологічному тиску на нього. Така ситуація має використовуватися з метою маніпулювання судовою думкою, сфальсифікованими доказовими базами по кримінальним провадженням сторонами як обвинувачення, так і захисту [154].

Однією з головних проблем сьогодення при проведенні СКТЕ є питання підтвердження компетентності осіб, які проводять даний вид експертиз, які володіють спеціальними знаннями в галузі інформації та які не є співробітниками державних судово-експертних установ [60, с. 144].

Для успішної боротьби з шахрайством в сфері банківських електронних платежів поряд з розробкою методичного забезпечення для виконання експертних досліджень, необхідне проведення регулярних міжнародних зустрічей представників правоохоронних органів. Метою цих зустрічей, повинна бути конкретизація основних напрямків даного виду діяльності і обмін досвідом, а також взаємодії у боротьбі з як внутрішньодержавними, так і міжнародними злочинними групами, що спеціалізуються на протиправних діяннях в області інформаційних технологій [72, с. 140].

Висновки до розділу 3

Під час дослідження організаційно-тактичних особливостей проведення окремих СРД, НСРД та інших процесуальних можна зробити наступні висновки:

1. На основі аналізу зазначених матеріалів, визначено, що мають місце наступні СРД: огляд місця події (59 %); допит потерпілого або представника потерпілої сторони (100 %); огляд ЕОТ, документів (85 %); освідування (1 %); допит свідка (14 %); допит підозрюваного (87 %); обшук (58 %); призначення судових експертиз (100 %); слідчий експеримент (6 %); пред'явлення особи для впізнання (5 %); одночасний допит раніше допитаних осіб (18 %).

2. Вказано, що по досліджуваній категорії кримінальних проваджень найбільш розповсюдженими СРД є допит потерпілого або представника потерпілої сторони, підозрюваного; призначення судових експертиз; огляд місця події, огляд ЕОТ, документів; обшук.

3. Вказується, що для збирання інформації з особистісних джерел необхідно проводити допити відповідних категорій осіб: потерпілого, свідка підозрюваного. Визначено категорії свідків. Встановлено, що підозрюваному у вчиненні шахрайства в сфері використання банківських електронних платежів необхідно ставити певні категорії питань: за яких обставин вчинено шахрайські дії; які способи застосовувалися (використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, які викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, з персональних комп'ютерів користувачів); які місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); які засоби використовувалися

при скоєнні правопорушення: це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації); яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчинення протиправних дій; який був порядок розподілу грошових коштів у членів ОГ чи ЗО; протягом якого періоду вчинялись протиправні діяння; які супутні кримінальні правопорушення було вчинено.

4. На основі вивчення матеріалів кримінальних проваджень, нами було встановлено, що специфічною ознакою досліджуваної категорії протиправних діянь є потреба проведення цілого ряду НСРД та оперативно-технічних заходів, пов’язаних із встановленням шахрая та його зв’язків. Зокрема, серед них було виокремлено такі як спостереження за об’єктом, огляд кореспонденції, прослуховування телефонних переговорів, зняття інформації з транспортних та електронних систем.

5. Надано характеристику особливосте призначення окремих видів експертиз.

ВИСНОВКИ

У дисертаційному дослідженні проведено теоретичний розгляд і вирішення наукового завдання з опрацювання та наукового обґрунтування концептуальних основ методики розслідування шахрайства у сфері використання банківських електронних платежів. Найбільш важливими результатами дисертації є наступні:

1. Визначено структуру криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів, яка нараховує наступні елементи: спосіб учинення шахрайства, обстановка вчинення кримінального правопорушення, слідова картина, особа шахрая та особа потерпілого. Встановлено, що вказані складові мають сталі кореляційні зв'язки та важливе значення для початкового етапу кримінального провадження з огляду на можливість висунення відповідних версій, а також проведення ряду слідчих та негласних слідчих (розшукових) дій.

2. Систематизовано способи вчинення вказаного протиправного діяння виходячи з того, що дана складова містить підготовку, безпосереднє вчинення та приховування протиправного діяння. На основі аналізу опитування працівників правоохоронних органів було встановлено, що мали місце такі підготовчі заходи до вчинення шахрайства у сфері банківських електронних платежів: підготовка відповідної електронно-обчислювальної техніки (комп'ютер, ноутбук, планшет тощо); створення програмного забезпечення для вчинення окремих видів шахрайства; вибір об'єкта, що буде предметом шахрайських дій; вибір кола осіб, які стануть жертвами шахрайських дій. Серед найбільш розповсюджених способів безпосереднього вчинення досліджуваного виду шахрайства під час користування онлайн-банкінгом, мобільним зв'язком, послугами в Інтернет-магазинах, визначено фішинг, сніфферінг, вішинг, кардинг. Визначено способи приховування кримінального правопорушення.

3. З’ясовано зміст обстановки та слідової картини вчинення шахрайства у сфері використання банківських електронних платежів. Зокрема, під час учинення такого шахрайства дії шахраїв можуть складатися із ряду операцій, пов’язаних із втручанням у облікові записи, електронні скриньки та інші електронні ресурси користувачів мережі Інтернет, які тривають у часі та здійснюються на необмеженій території. У зв’язку із чим набуває актуальності встановлення часово-просторових характеристик вчинення шахрайських дій. Часові параметри є достатньо розпливчасті, втім часом вчинення шахрайства у сфері електронних банківських платежів слід вважати момент проведення транзакції, завдяки якій потерпілого було позбавлено грошей на його рахунку. У фізичному сенсі місцями вчинення шахрайства у сфері банківських електронних платежів, можуть бути: місця знаходження комп’ютерної техніки, із якої здійснюються шахрайські дії (стаціонарне комп’ютерне обладнання, ноутбук (телефон, планшет), що переміщується у просторі і підключений до мережі Інтернет) – 78 %; місця знаходження банкоматів, банків, з яких знімалася готівка – 56 %; місце знаходження потерпілого, який виявив шахрайські дії при здійсненні електронних платежів – 67 % тощо. Утім, обстановку вчинення даного шахрайства слід розглядати і як віртуальний простір, в якому передається, зчитується та змінюється електронно-цифрова інформація, завдяки якій здійснюється втручання в облікові записи користувачів мережі Інтернет та знімаються грошові суми внаслідок незаконних транзакцій. До складу обстановки вчинення шахрайства у сфері використання банківських платежів запропоновано віднести й систему інформаційних ресурсів, пов’язаних із функціонуванням платіжних систем, через які проводяться транзакції та рівень інформаційної безпеки у банківській сфері.

Слідова картина шахрайств у сфері електронних банківських платежів включає 3 групи слідів: 1) матеріальні сліди, що відображаються у квитанціях та роздруківках про електронні банківські платежі (68 %); на банківських картках (46 %); на сім-картках (37 %); на паперових копіях

комп’ютерної інформації (44 %); сліди папілярних ліній на засобах комп’ютерної техніки, клавіатурі терміналу (17 %) тощо; 2) ідеальні сліди, що складають 28 % і відображаються у пам’яті потерпілих та осіб, які були свідками незаконних операцій із банківськими платежами з боку шахраїв; 3) віртуальні сліди (електронно-цифрові), що займають домінуюче місце і містяться: у пам’яті мобільного телефону (IMEI-код; історія телефонних з’єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо) – 88 %; на сервері мобільного оператора – 76 %; на сервері інтернет-провайдера (сервер зберігання flow-статистики и биллінгової інформації, сервер баз даних тощо) – 67 %; у пам’яті сім-карти – 79 %; у пам’яті комп’ютерів, планшетів – 92 %; у електронній поштовій скриньці – 56 %; на флеш карті (файли, папки тощо) – 34 %; дані електронного журналу банкомату (терміналу) – 29 %; інформація в електронному вигляді, яка відображає суми грошових коштів, переказаних через певну систему електронних платежів («Приват-банк», “Qiwi-гаманець”, MoneyGram, Western Union, Perfect Money та ін.) – 48 %; профіль у соціальних мережах, інформація на сайтах – 42 % тощо.

4. Надано характеристику особи шахрая, а саме визначено, що шахрайства в сфері 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.

Виокремлено віктимогенні групи потерпілих, а саме: 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.

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

6. Сформульовано типові слідчі ситуації розслідування досліджуваного виду шахрайства, зокрема: 1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай відомий – 19 %; 2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %; 3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %; 4) вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %.

7. Виокремлено організаційно-тактичні аспекти проведення окремих СРД, спрямованих на отримання інформації з матеріальних та особистісних джерел. Зазначено, що шахрайства у сфері використання електронних банківських платежів як правило здійснюються за допомогою спеціальних програм, що маскують реальне місце знаходження особи шахрая так званих анонімайзерів таких як VPN – скорочена назва від англ. Virtual Privat Network – віртуальна приват мережа, Socks скорочена назва від англ. Socked Secure – мережевий протокол та ін. Здебільшого такі протиправні діяння вчиняються або ОГ, або ЗО. Визначено категорії свідків при розслідуванні досліджуваної категорії протиправних діянь, а саме: особи, яким може бути відома інформація про обставини та умови протиправної діяльності, яку вони спостерігали; особи, які перебувають у родинному або іншому зв’язку із шахраєм; особи, яким відомо умови та обставини тих дій, в яких вони брали участь; особи, які певним чином сприяли вчиненню шахрайства, але самі про це не знали; особи, які були обізнані про обставини, що передували шахрайству; працівників банківських установ, що були задіяні в використанні банківських електронних платежів.

Установлено, що підозрюваному у вчиненні шахрайства в сфері використання банківських електронних платежів необхідно ставити певні

категорії питань: за яких обставин вчинено шахрайські дії; що за способи застосовувалися (використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, що були викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, із персональних комп'ютерів користувачів); які місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання шахрайських програм, технічних прийомів); які саме засоби використовувалися під час скоєння правопорушення, – це можуть бути як технічні, такі як ЕОТ, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації); яка саме загальна сума матеріальних цінностей або грошових коштів утворилась у результаті вчинення протиправних дій; який був порядок розподілу грошових коштів у членів ОГ чи ЗО; протягом якого періоду вчинялись протиправні діяння; що за супутні кримінальні правопорушення було вчинено.

Охарактеризовано організаційно-тактичні особливості проведення обшуку та огляду. Зокрема, вказано, що обшук здебільшого проводився в місцях: зберігання й обробки інформації щодо банківських електронних платежів, що зазнала злочинного впливу (67 %); знаходження комп'ютерного обладнання, що використовувалося у процесі здійснення протиправного діяння (43 %); збереження інформації, отриманої злочинним шляхом (41 %); настання шкідливих наслідків (10 %). Під час огляду електронних інформаційних систем (комп'ютер, планшет, мобільний телефон, тощо) об'єктом огляду є така техніка, а також носії інформації (наприклад, IP-адреси, системні дані, програми, cookies браузерів, КЕШ тощо).

8. З'ясовано організацію і тактику проведення окремих НСРД при розслідуванні шахрайства в сфері банківських електронних платежів. На

основі вивчення матеріалів кримінальних проваджень, було встановлено, що специфічною ознакою досліджуваної категорії протиправних діянь є потреба проведення цілого ряду НСРД та оперативно-технічних заходів, пов’язаних із встановленням шахрая та його зв’язків. Зокрема, серед них було виокремлено такі як спостереження за об’єктом, огляд кореспонденції, прослуховування телефонних переговорів, зняття інформації з транспортних та електронних систем.

9. Конкретизовано особливості призначення експертиз у кримінальних провадженнях вказаної категорії. Зокрема, під час проведення підвиду СКТЕ експерту необхідно зупинитися на таких моментах: виявити відношення досліджуваної техніки до апаратних комп’ютерних засобів; визначити тип, марку або модель даного пристрою; встановити технічні характеристики і параметри досліджуваного технічного засобу; визначити первинну конфігурацію і характеристики даного пристрою, а також дізнатись, чи було змінено його функціональні властивості порівняно з первісною конфігурацією; провести зовнішній огляд техніки стосовно фізичного втручання у його конфігурацію; встановити, чи є цей технічний засіб накопичувачем інформації, та чи відкритий доступ до такої інформації.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Абушов Т. А. Система організаційних і тактичних дій під час проведення обшуку. *Науковий вісник Національної академії внутрішніх справ*. № 6. 2011. С. 198–205.

2. Авдєєва Г. К. Сутність цифрових слідів в криміналістиці. *Актуальні питання судової експертизи та криміналістики* : зб. матеріалів Міжнар. наук.-практ. конф., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90–93.

3. Авдєєва Г. К., Стороженко С. В. Електронні сліди : поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. Вип. 1 (77). С. 169–176.

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

5. Аленин Ю. П. О структуре методики расследования преступлений. *Юридична освіта і правова держава (до 150-річчя юридичного ін-ту ОДУ)*: Зб. наук. праць. Одеса : Астропринт. 1997. С. 244–250.

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

7. Анапольська А. І. Розслідування шахрайств і пов’язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків: дис. ... канд. юрид. наук: спец. 12.00.09 / Луганський державний університет внутрішніх справ ім. Е.О. Дідоренка. Луганськ. 2010. 243 с.

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

9. Багатостороння загроза шахрайства: чи готові банки гідно протистояти виклику. Глобальне дослідження з питань шахрайства у банківській сфері. URL: https://assets.kpmg/content/dam/kpmg/ua/pdf/2020/01/Global-Banking-Fraud-Survey.pdf (дата звернення 01.09.2021).

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

11. Бахин В. П. Криминалистика. Проблемы и мнения (1962-2002) / К.: Типография журнала «Охрана труда», 2002. 268 с.

12. Бедь В. В. Юридична психологія: Навчальний посібник / К : «Каравелла»; Львів : «Новий світ-2000», «Магнолі плюс» 2003. 376 с.

13. 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.

14. Безруков Д. В. Використання технічних засобів підрозділами карного розшуку у протидії злочинам: історичний аспект. *Проблеми правознавства та правоохоронної діяльності*. 2015. № 1 (52). С. 163–174.

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

16. Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.

17. Білоус О. В. Законодавча регламентація проникнення до житла чи іншого володіння особи під час кримінального провадження. *Держава і право. Збірник наукових праць. Юридичні і політичні науки*. Випуск 65. К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2014. С. 264–271.

18. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних

злочинів: автореф. дис. … на здобуття наук. ступеня канд. юрид. наук: 12.00.09. Київський національний університет імені Тараса Шевченка. Київ, 2008. 20 с.

19. Богинский В. Е. Система тактических приемов допроса подозреваемого: автореф. дис… канд. юрид. наук: 12. 00. 09 / ХЮрИ. Харьков, 1980. 18 с.

20. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

21. Буров Є. В. Комп'ютерні мережі: підручник / Львів : «Магнолія 2006», 2010. 262 с.

22. Валуйская М. Ю. К вопросу о типологии лиц, совершивших умышленные убийства при отягчающих обстоятельствах. *Вісник Луганського інституту внутрішніх справ МВС України: Наук. теоретич. журнал*. 2000. Вип. 2. С. 138–145.

23. Вапнярчук В. В. Досудове провадження. Глава 14. *Кримінальний процес* : підручник / [Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін.] ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. С. 334.

24. Венедіктов А. А. Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації в оперативно-розшуковій діяльності та кримінальному процесі. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 74–77.

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

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

27. Гетьман А. Науково-практичний коментар нового Кримінального процесуального кодексу України від 13 квіт. 2012 р. № 4651-VI. URL: http://www.yport.inf.ua/stattya-sposterejennya-osoboyu-richchyu-abo-50510.html. (дата звернення – 14.04.2021)

28. Головіна В. П. Основи методики розслідування легалізації (відмивання) грошових коштів, здобутих злочинних шляхом, з використанням кредитно-банківської системи: дис. … канд. юрид. наук: 12.00.09 / Національна академія внутрішніх справ України. Київ, 2004. 178 с.

29. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2008. 18 с.

30. Головкін С. В. Особливості тактики допиту підозрюваного в скоєнні шахрайства. *Вісник Луганського державного університету внутрішніх справ*. 2007. Спеціальний випуск № 2, частина 3. Луганськ: РВВ ЛДУВС. С. 75–78.

31. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: монографія. Запоріжжя, 2003. 250 с.

32. Гора И. В. Организационные проблемы судебно-экспертной деятельности в Украине. *Criminalistics and forensic expertology: science, studies, practice*. Vilnius, Varsuva. 2016. С. 263–278.

33. Грібов Л. М., Пугач С. М. Технічні засоби, що використовуються під час проведення негласних слідчих (розшукових) дій. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2 (33). С. 3–6.

34. Давыдов В. О., Головин А. Ю. Значение виртуальных следов в расследовании преступлений экстремистского характера. *Экономические и юридические науки*. 2016. № 3. С. 254–259.

35. Департамент кіберполіції Національної поліції України: офіційний сайт. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення –

19.10.2019)

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

37. ДП: Доверие, доставка, мошенники: как пандемия изменила онлайн-платежи. URL: https://www.reksoft.ru/blog/2020/09/07/koronavirus-online-prodazhi/ (дата звернення – 21.08.2021)

38. Дубно Т. В. Взаємозв'язок обстановки та часу вчинення злочину. *Науковий вісник Львівського державного університету внутрішніх справ*. 2012. № 3. С. 375–383.

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

40. Експертизи у судочинстві України: науково-практичний посібник/ заг.ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2014. 504 с.

41. Експертна служба МВС України дотримання прав і свобод особи під час проведення обшуку при розслідуванні кримінальних URL: https://dndekc.mvs.gov.ua/ (дата звернення – 22.09.2021)

42. Електронна комерція в Україні. Статистика за 2015–2016 рр. URL: http://nuigde.biz/uk/ blog/elektronnaya-kommerciya-v-ukraine-statistika-za-2015-2016-goda.html (дата звернення 12.09.2021).

43. URL: https://www.ema.com.ua/citizens/wiki/karding/ (дата звернення – 07.10.2021)

44. Єфімов М. М. Пріоритетні напрями розслідування злочинів проти моральності в розрізі євроінтеграційних процесів. *Інновації юридичної науки в євроінтеграційному процесі*: матеріали Міжнародної наук.-практ. конф. (10–11 березня 2017 року, м. Сладковічево). Словацька Республіка. Університет Данубіус, юридичний факультет Янко Єсенського. 2017. С. 268–271.

45. 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.

46. Жордания И. Ш. Психолого-правовая структура способа совершения преступления / Тбилиси: Изд-во «Сабчота Сакартвело», 1977. 233 с.

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

48. Журавель В. А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія та практика судової експертизи і криміналістики*. Харків : Право, 2008. Вип. 8. С. 152–159.

49. Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю: автореф. дис. … канд. юрид. наук: спец.: 12.00.09 – кримінальний процес та криміналістика; судова експертиза / 20 с.

50. Зарубей В. В., Ілляшенко О. В. Особливості висунення та планування версій при розслідуванні квартирних крадіжок, вчинених іноземцями. *Сучасний стан криміналістичного забезпечення досудового розслідування*: збірник матеріалів конференції (20 квітня 2017 року). Київ : Навчально-науковий інститут № 2 Національної академії внутрішніх справ, 2017. С. 139–142.

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

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

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

54. Ілляшенко С. М., Іванова Т. Є. Перспективи та основні проблеми

розвитку інтернет-торгівлі в Україні. *Механізм регулювання економіки*. 2014. № 3. С. 113–119.

55. Інструкція про призначення та проведення судових експертиз та експертних досліджень : затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення – 22.09.2021)

56. Іщенко А. В. Фундаментальні та прикладні криміналістичні категорії. *Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах*: Міжнародна науково-практична конференція 5 листопада 2010 р., м. Запоріжжя: матеріали у 3 част. Запоріжжя. 2010. ч.1. С. 180–182.

57. Калюга Т. О., Чаплинський К. О. Теоретичні та практичні основи розслідування шахрайства у сфері надання туристичних послуг : монографія. Херсон : Видавничий дім «Гельветика», 2020. 238 с.

58. Кант И. Трактаты и письма / пер. с нем. М.: Наука, 1980. 286 с.

59. Кардинг. URL: https://uk.wikipedia.org/wiki/Кардинґ (дата звернення – 07.10.2021)

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

61. Керевич О. В. Особливості проведення окремих невідкладних негласних слідчих (розшукових) дій. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 101–105.

62. Кібератаки на Україну коштують мільйони доларів – СБУ / URL: https://detector.media/infospace/article/122774/2017-02-02-kiberataky-na-ukrainu-koshtuyut-milyony-dolariv-sbu/ (дата звернення – 20.06.2021)

63. Кіберполіція встановила факт шахрайського заволодіння грошима банку : Департамент кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vstanovyla-fakt-shaxrajskogo-zavolodinnya-groshyma-banku-8388/ (дата звернення – 10.10.2021)

64. Кіберполіція Дніпропетровщини викрила зловмисників у

привласненні грошей іноземців за допомогою фішингу : Департамент кіберполіції Національної поліції України. URL: https://mvs.gov.ua/uk/press-center/news/kiberpoliciya-dnipropetrovshhini-vikrila-zlovmisnikiv-u-privlasnenni-grosei-inozemciv-za-dopomogoyu-fisingu (дата звернення – 22.07.2021)

65. Кіпа О. О. Правопорушення в мережі Інтернет. *Часопис Київського університету права*. 2010. № 4. С. 346–349

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

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

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

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

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

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

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

72. 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.

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

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

75. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

76. Коваль Н. О., Борщ М. В. Особливості функціонування платіжних систем Україні на сучасному етапі їх розвитку. *Електронний журнал* «*Ефективна економіка»*. 2012. № 10. URL: http://www.economy. nayka.com.ua/images/top_plashka.jpg (дата звернення 01.08.2021).

77. Колесник В. А. Негласні слідчі (розшукові) дії: кримінально-процесуальні та криміналістичні аспекти підготовки і проведення : науково-практичний посібник / Академія адвокатури України. Київ : Прецедент, 2014. 135 с.

78. Колесник В. А. Суб'єкти здійснення та класифікація негласних слідчих (розшукових) дій. *Юридичний часопис Національної академії*

внутрішніх справ. 2013. № 1. С. 129–134.

79. Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений. Учеб. пособие. Харьков : Юрид. ин-т, 1985. 93 с.

80. Колесниченко А. Н. Общие положения методики расследования отдельных видов преступлений. Текст лекции. Харьков : Харьк. юрид. ин-т. 1976. С. 9–11.

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

82. Комп'ютерно-технічна експертиза. URL: https://www.hniise.gov.ua/13973-kompyuterno-texnchna-ekspertiza.html (дата звернення – 14.10.2021)

83. Коновалова В. Е. Допрос: тактика и психология: моногр. Харьков : Изд-во СПД ФЛ Вапнярчук Н.Н., 2006. 176 с.

84. Коновалова В. Е. Тактика допроса свидетелей и обвиняемых / Харків : Изд-во ХГУ, 1956. 129 с.

85. Конституція України // Відомості Верховної Ради України (ВВР). 1996. № 30. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення – 08.08.2021)

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

87. 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.

88. Коршикова Т. В. Типові слідчі ситуації та програми дій слідчого на початковому етапі розслідування шахрайств, учинених з використанням

електронно-обчислювальної техніки. *Південноукраїнський правничий часопис.* 2020. Вип. 4. С. 123–131.

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

90. Кравченко О. В. Психологічні особливості шахрайства: автореф. дис. ... канд. психол. наук: спец. 19.00.06 / Нац. ун-т внутр. справ. Харків, 2005. 21 с.

91. Криміналістика: підручник / [В. Д. Берназ, В. В. Бірюков, А. Ф. Волобуєв та інші]; за заг. ред. А. Ф. Волобуєва. Харків : ХНУВС, 2011. 468 с.

92. Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і доп. Харків : Право, 2008. 464 с.

93. Криміналістика : Підручник для студ. юрид. ВНЗ / Кол. авт. Глібко В. М., Дудніков А. Л., Журавель В. А. та ін. / За ред. В. Ю. Шепітька. К.: Видавничій Дім «Ін Юре», 2001. 452 с.

94. Криміналістика. Криміналістична тактика і методика розслідування злочинів: Підруч. для студентів юрид. вузів і фак. / За ред. В.Ю. Шепітька. Харків : Право, 1998. 366 с.

95. Кримінальне право. Загальна частина : підручник / за ред. А. С. Беніцького, В. С. Гуславського, О. О. Дудорова, Б. Г. Розовського. Київ : Істина, 2011. 1121 с.

96. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14/page#Text (дата звернення – 11.07.2021)

97. Кримінальний процесуальний кодекс України від 13.04.2012

№ 4651-VI. Офіційний сайт ВР України. URL: http://zakon4.rada.gov.ua/laws/show/4651-17 (дата звернення – 20.04.2021)

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

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

100. Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриценко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні: Навчально-практичний посібник. Харків : «Оберіг», 2013. 344 с.

101. Кудрявцев В. Н. Способ совершения преступления и его уголовно-правовое значение. *Сов. государство и право*. 1957. № 8. С. 60–69.

102. Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. Теорія і практика *:* навч. посіб. Київ : КНТ, 2008. 248 с.

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

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

105. Курман А. В. Мошенничество с финансовыми ресурсами: проблемы криминалистической теории. *Проблеми законності*: Респ. міжвідом. наук. зб. / Відп. ред. В. Я. Тацій. Харків : Нац. юрид. акад. України, 2000. Вип. 44. С. 215–219.

106. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : автореф. дис. … к-та юр. наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого, Харків, 2002. 16 с.

107. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : дис. ... канд. юрид. наук: 12.00.09 / Національна юридична академія України ім. Ярослава Мудрого. Харків, 2002. 227 с.

108. Курс сучасної української кримінології: теорія і практика : у 3 кн. К. : Видавничий Дім «Ін Юре», Кн. 1 : Теоретичні засади та історія української кримінологічної науки. 2007. 424 с.

109. Лисиченко В. К., Гончаренко В. И., Салтевский М. В. Советская криминалистика. Методика расследования отдельных видов преступлений / Київ : Вища школа. Головное изд-во, 1988. 384 с.

110. Лысенко В. В. Расследование уклонений от уплаты налогов, совершенных должностными лицами предприятий, организаций, учреждений. Харків : Фирма «Консум», 1997. 192 с.

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

112. Малышкин П. В. Способ сокрытия преступления и его место в структуре способа совершения преступления. *Следователь*. 2009. № 1. С. 19–24.

113. Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков : Консум, 1999. 480 с.

114. Методика расследования отдельных видов преступлений / В. К. Лисиченко, В. И. Гончаренко, М. В. Салтевський и др.; под. ред. В.К. Лисиченко. Киев : Выща шк. Головное изд-во, 1988, 405 с.

115. Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ: навчальний посібник / [О.В. Батюк, Р.І. Благута, О.М. Гумін та ін.]; за заг. ред. Є.В. Пряхіна. Львів : ЛьвДУВС, 2011. 324 с.

116. Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення

зберігання інформації про клієнтів об'єктами платіжної інфраструктури. URL: https://bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi (дата звернення – 12.09.2021)

117. Мусиенко О. Л. Особенности допроса обвиняемых при расследовании мошенничества. *Право обвинуваченого на кваліфікований захист та його забезпечення*: Матеріали міжнар. наук.-практ. семінару, 1–2 груд. 2005 р.; Харків / Редкол.: В. В. Сташис та ін. Харків ; Київ : ЦНТ Гопак, 2006. С. 214–216.

118. Мусиенко О. Л. Сущность мошенничества, его виды и формы. *Актуальні проблеми держави та права: Зб. наук. праць*. Одеса: Астропрінт, 1998. Вип. 5. С. 90–96.

119. Мусієнко О. Л. Допит свідків при розслідуванні шахрайства. *Проблеми законності*: Респ. міжвідом. наук. зб. / Відп. ред. В. Я. Тацій. Харків : НЮАУ, 2007. Вип. 91. С. 156–161.

120. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : автореф. дис. … к-та юр. наук : 12.00.09 / Національна юридична академія України імені Ярослава Мудрого: Харків, 2007. 18 с.

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

122. Науково-практичний коментар до кримінального кодексу . Радник. Український юридичний портал. URL: http://radnuk.info/komentar/kruminal/osobluva/302-rozd16/4662--361html. (дата звернення 12.10.2021)

123. Науково-практичний коментар кримінального кодексу України від 5 квітня 2001 року / [за ред. М. І. Мельника, М. І. Хавронюка]. Київ : Каннон ; А.С.К, 2002. 1104 с.

124. Некрасов В. Атака по телефону: Україну накрила хвиля

кібершахрайства / Електронний ресурс : Режим доступу: https://www.epravda.com.ua/rus/publications/2017/01/30/619178/. (дата звернення – 12.09.2020)

125. Нескоромний Д. А. Проведення негласних слідчих (розшукових) дій працівниками СБ України при розслідуванні кримінальних правопорушень, вчинених організованими злочинними групами. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 20–23.

126. Олиндер Н. В. Типичные способы совершения преступлений с использованием электронных платежных средств и систем. *Эксперт-криминалист*. 2014. № 1. С. 13–16.

127. Олійник Я. О. Допит свідків, підозрюваних та обвинувачених під час розслідування умисного знищення або пошкодження об'єктів житлово-комунального господарства. URL: http://www.pravoznavec.com.ua/period/article/17551/%DE (дата звернення – 12.01.2021)

128. Омельяненко М. Особенности криминалистической характеристики Интернет-мошенничества URL: http://kpk.org.ua/2007/12/18/osobennosti-kriminalisticheskojj.html (дата звернення – 11.08.2021)

129. Опанасенко Н.О. Криміналістична характеристика та основні положення розслідування шахрайства, вчиненого організованими злочинними групами у сфері житлового будівництва : дис. на здоб. наук. ст. к.ю.н. / Академія адвокатури України. Київ. 2018. 253 с.

130. Оперативно-розшукова діяльність : навч. посіб. / Є. М. Моісеєв, О. М. Джужа, Д. Й. Никифорчук [та ін.]; За ред. проф. О. М. Джужи. Київ : Правова єдність, 2009. 310 с.

131. Офіційний сайт NORTON / URL: https://us.norton.com/cyber-security-insights-2017 (дата звернення – 12.01.2021)

132. Офіційний сайт Департаменту кіберполіції Національної поліції України / URL : https://cyberpolice.gov.ua/ (дата звернення – 12.01.2021)

133. Охрімчук Т. В. Криміналістична характеристика шахрайства з

фінансовими ресурсами. *Боротьба з організованою злочинністю і корупцією (теорія і практика). Науково-практичний журнал*. № 23. 2010. С. 369–374.

134. Охрімчук Т. В. Криміналістична характеристика шахрайства з фінансовими ресурсами та основні напрями розслідування : автореф. дис. … к-та юр. наук : 12.00.09 / Національна академія внутрішніх справ. Київ, 2011. 16 с.

135. Охрімчук Т. В. Особливості використання спеціальних знань при розслідуванні шахрайства з фінансовими ресурсами. *Фінанси, економіка, право*. 2010. № 8. С. 59–63.

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

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

138. Павлова Н. В. Особливості розслідування шахрайства, пов’язаного з відчуженням приватного житла: дис... канд. юрид. наук: 12.00.09 / Дніпроп. держ. ун-т внутр. справ. Дніпропетровськ, 2007. 223 с.

139. Павлова Н. В. Розслідування шахрайства при укладанні цивільно-правових угод щодо відчуження житла: монографія. Дніпропетровськ : ДДУВС, 2008. 176 с.

140. Павлова Н. В. Щодо важливості правопорушень, вчинених шляхом шахрайства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. № 1. С. 190–196.

141. Пазиніч В. І. Особливості порушення кримінальної справи і початкового етапу розслідування злочинів, які пов’язані з втручанням в роботу мереж мобільного зв’язку. *Науковий вісник Іменем закону*. 2007. № 2.

С. 27–29.

142. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: автореф. дис. … канд. юрид. наук: 12.00.09 / Академія прокуратури. Київ, 2005. 21 с.

143. Пиріг І. В. Фіксація результатів дослідницької діяльності спеціалістів на місці події. *Криміналістика і судова експертиза*: міжвідом. наук.-метод. зб. Київський НДІ судових експертиз; редкол.: О. Г. Рувін (голов. ред.) та ін. Київ, 2020. Вип. 65. С. 220–229.

144. Пиріг І. В. Організація і тактика проведення огляду місця події у сучасних умовах розвитку науки і техніки. *Криміналістичний вісник*: наук.-практ. зб. / [редкол.: І.М. Охріменко (голов. ред.) та ін.]; ДНДЕКЦ МВС України; НАВС. Київ : ДНДЕКЦ МВС України, 2019. № 2 (32). С. 30–37.

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

146. Погорецький М. А., Сергєєва Д. Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 137–141.

147. Преловський К. В. Сутність і зміст поняття критичної інфраструктури банківської системи України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2018. № 2. С. 94–98.

148. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII. URL: zakon2.rada.gov.ua/laws/show /675-19 (дата звернення – 14.06.2021)

149. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : Спільний наказ ГПУ, МВС, СБУ, Адміністрації ДПрС, МФ, МЮ № 114/1042/516/1199/936/1687/5 від 16.11.2012 р. URL:

https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення – 15.07.2021)

150. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 34. URL: http://zakon5.rada.gov.ua/laws/show/2297-17 (дата звернення 20.04.2021)

151. Про оперативно-розшукову діяльність: Закон України від 22.05.2019р. № 2720-VIII. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення – 12.01.2021)

152. Про платіжні системи та переказ коштів в Україні: Закон України від 5 квітня 2001 року. URL: https://zakon.rada.gov.ua/laws/main/index (дата звернення 12.09.2021)

153. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення – 22.09.2021)

154. Проблемы проведения и научного обеспечения судебных экспертиз / URL: https://ceur.ru/library/articles/ pravo/item127028. (дата звернення – 15.10.2021)

155. Пчеліна О. В. Тактичні операції під час розслідування злочинів у сфері службової діяльності. *Підприємництво, господарство і право*. 2017. № 3. С. 290–294.

156. Пчеліна О. В., Корнієнко В. В. Особливості розслідування злочинів, вчинених шляхом кредитнофінансових операцій: Методичні рекомендації. Харків : Харківській нац. ун-т внутр. справ, 2011. 36 с.

157. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку: дис. … канд. юрид. наук: 12.00.08. Дніпровський національний університет імені Олеся Гончара, Дніпро; Університет державної фіскальної служби України, Ірпінь, 2019. 208 с.

158. Сазонов М. М. Виды мошенничеств с банковскими картами и

совершенствование мер виктимологического предупреждения. *Виктимология*. 2018. № 2 (16). С. 55–60.

159. Салтевський М. В. Криміналістика (у сучасному викладі); Підручник. Київ : Кондор, 2005. 588 с.

160. Салтевський М. В. Криміналістика. Підручник: У 2-х ч. Ч. 1. Харків : КонСУМ ; Основа, 1999. 416 с.

161. Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2018. Т. 29 (68). № 4. С. 165–169.

162. Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* 2015. № 4. С. 408–411.

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

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

165. Самойленко О. А. Типізація особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору (з позицій криміналістичної науки). *Підприємництво, господарство і право*. 2018. № 8. С. 195–201.

166. Самойлов С. В. Особенности истребования следователем сведений при расследовании мошенничества, совершенного с использованием сети Интернет. *Вопросы криминологии, криминалистики и судебной экспертизы*. 2013. № 2 (34). С. 97–101.

167. 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 (03). С. 82–86.

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. Самойлов С. В. Способы совершения мошенничества, связанного с куплей/продажей с использованием сети Интернет (криминалистический аспект). *Закон и жизнь*. 2013. № 8/3 (260). С. 175–179.

171. Самойлов С. В. «Фішинг» як спосіб вчинення Інтернет-шахрайств. *Актуальні питання сучасних державотворчих та правотворчих процесів*: матеріали міжнар. наук.-практ. конф. (м. Запоріжжя, 24 лютого 2011 р.), у 3-х частинах. Запоріжжя : Запорізька міська громадська організація «Істина», 2011. Ч. 3. С. 102–104.

172. Самойлов С. В., Одерій О. В. Застосування спеціальних знань під час розслідування шахрайств, учинених з використанням мережі Інтернет. *Криміналістичний вісник*. 2012. № 2 (18). С. 106–113.

173. Севідов О. А. Криміналістична класифікація суб'єктів кіберзлочинів та їх особливості. *Актуальні питання розслідування кіберзлочинів*: матеріали Міжнар. наук.-практ. конф. (м. Харків, 10 груд. 2013 р.). Харків : ХНУВС, 2013. С. 164–169.

174. Селезньова О. М. Теоретико-методологічні основи інформаційного права України: монографія. Чернівці : Місто, 2014. 407 с.

175. Селецький С. І. Кримінальне право України. Загальна частина. Київ : Центр учбової літератури, 2008. 248 с.

176. Сергєєва Д. Б. Результати негласних слідчих (розшукових) дій: проблемні аспекти визначення. *Право і громадянське суспільство*. 2014. № 1. С. 97–106.

177. Сіренко О. В. Обстановка вчинення крадіжок, грабежів і розбійних нападів неповнолітніми як елемент криміналістичної характеристики. *Науковий вісник Національного університету ДПС України*

(економіка, право). № 4 (59). 2012. С. 223–228.

178. Слепухина А. С. Компьютерные информационные технологии : курс лекций. Витебск : МИТСО, 2009. 201 с.

179. Слободзян А. Нормативно-правове регулювання діяльності суб'єктів негласних слідчих (розшукових) дій. *Вісник Національної академії прокуратури України*. № 2 (35). 2014. С. 86–91.

180. Сорокіна Л. В. Особа злочинця, яка вчиняє злочини у сфері пенсійного забезпечення. *Правовий часопис Донбасу.* № 1 (66). 2019. С. 99–106.

181. Справа № 350/184/18. Архів Рожнятівського районного суду Івано-Франківської обл., 2018 р.

182. Справа № 463/7254/21. Архів Личаківського районного суду м. Львова, 2021 р.

183. Старушкевич А. В. Криміналістична характеристика злочинів : Навч. посібник. Київ, 1997. 44 с.

184. Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека*. 2013. № 3 (50). С. 110–115.

185. Степанюк Р. Л. Сутність і практичне значення криміналістичної характеристики злочинів. *Порівняльно-аналітичне право.* 2014. № 5. С. 398–400.

186. Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 41–49.

187. Табак И. С. Мошенничество с банковскими картами. *Современные инновации*. 2018. № 4 (26). № 1 (19). С. 37–40.

188. 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.

189. Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : дис. … д-ра юрид. наук : 12.00.09 / Одеса, 2003. 276 с.

190. Тіщенко В. В. Криміналістичні технології в теорії і практиці розслідування. *Актуальні проблеми держави і права*: зб. наук. праць. Вип. 44. Одеса : Юридична література, 2008. С. 18–24.

191. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

192. Топорецька З. М. Слідова картина як джерело первинної інформації про вчинення злочинів у сфері грального бізнесу. *Реформування національного та міжнародного права: перспективи та сьогодення*: матеріали Міжнародної науково-практичної конференції (м. Одеса, Україна, 29-30 вересня 2011 р.) у 2-х ч. Одеса : ГО «Причорноморська фундація права», 2011. Ч. 2. С. 105–108.

193. У Києві кіберполіція викрила факт шахрайського заволодіння нерухомістю за допомоги комп'ютерного вірусу : Департамент кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/u-kyyevi-kiberpolicziya-vykryla-fakt-shaxrajskogo-zavolodinnya-neruxomistyu-za-dopomogy-kompyuternogo-virusu-3654/ (дата звернення – 10.10.2021)

194. Уголовный кодекс Украины : науч.-практ. коммент. / отв. ред. Е. Л. Стрельцов. 6-е изд., перераб. и доп. Харьков : Одиссей, 2009. 888 с.

195. Узунова О. В., Калюга К. В. Проблеми прийомів аналізу отриманої з місця події інформації та обґрунтування припущень стосовно особи злочинця. URL: http://bo0k.net/index.php?bid=18860&chapter=1&p=achapter (дата звернення – 28.11.2020)

196. Феоктистов М. В. Неправомерный оборот средств платежей. *Законность*. 2016. Вип. 1 (975). С. 45–48.

197. Фінагеєв В. О. Способи вчинення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків. *Науковий вісник Національної академії внутрішніх справ*. 2016. № 1. С. 63–82.

198. Франк Л. В. Виктимология и виктимность : учеб. пособие. Душанбе, 1972. 152 с.

199. Хамига Ю. Я. Фінансове шахрайство: критерії ідентифікації та напрями мінімізації : дис. … доктора філософії: Спеціальність 072 – Фінанси, банківська справа та страхування; Галузь знань 07 – Управління та адміністрування / Західноукраїнський національний університет. Тернопіль, 2020. 308 с.

200. Харчук М. В. Аналіз масштабів та основні напрями мінімалізації ризиків шахрайства членів міжнародних платіжних систем. *Електронний журнал «Ефективна економіка»*. 2013. № 6. URL: http://www.economy.nayka.com.ua/images/top_plashka.jpg (дата звернення 05.09.2021).

201. Хижняк Є. С. Типові слідчі ситуації при розслідуванні статевих злочинів. *Південноукраїнський правничий часопис*. 2012. № 4. С. 197–199.

202. Ціркаль В. В. Тактика проведення обшуку з участю фахівців. *Вісник. Серія «Юридичні науки»*. 2002. С. 45–48.

203. Чаплинський К. О. Організація і тактичні прийоми проведення одночасних обшуків. *Науковий вісник Юрид. академії Мін-ва внутр. справ*. 2004. № 3 (17). С. 338–344.

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

205. 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. 36 с.

206. 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.

207. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування: монографія. К. : Хай-Тек Прес, 2010. 620 с.

208. 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.

209. Чучко С. В. Оцінка первісної інформації та коло обставин, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет: окремі аспекти. *Наук. вісн. Дніпроп. держ. ун-ту внутр. справ.* № 3. 2020. С. 304–310.

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

211. Шапочка С. В. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет. *Правова інформатика*. 2014. № 3 (43). С. 89–95.

212. Шевчук В. М. Слідча ситуація: повнота, структура, види та її значення для оптимізації розслідування злочинів. *Юридичний науковий електронний журнал*. № 1. 2014. С. 142–150.

213. Шепитько В. Ю. Теория криминалистической тактики : монография. Харьков : Гриф, 2002. 218 с.

214. Яременко О. І. Сучасне право розуміння відносин в інформаційній сфері та методологія їх систематизації. *Інформація і право*. № 3 (22). 2017. С. 30–42.

215. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Електронне наукове фахове видання «Ефективна економіка*». URL : http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf (дата звернення – 17.08.2021)

216. Chuchko Sergey Fraud methods, related to purchase of goods through the Internet. *Науковий журнал «Visegrad Journal on Human Rights»*

(«Пан'європейський університет» Словацької Республіки). 6 (volume 3). 2019. P. 234–238.

217. IEEE Standards Association (IEEE SA) URL: https://standards.ieee.org/products-services/regauth/oui36/index.html (дата звернення – 21.09.2021)

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. Mihir Bellare Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. Springer Berlin Heidelberg, 2000. 274 p.

ДОДАТКИ

Додаток А

Результати вивчення
156 кримінальних справ та 211 кримінальних проваджень за фактами вчинення шахрайства у сфері використання банківських електронних платежів (Вінницька, Волинська, Дніпропетровська, Донецька, Запорізька, Кіровоградська, Київська, Львівська, Луганська, Миколаївська, Одеська, Полтавська, Тернопільська, Харківська, Херсонська області та м. Київ)

№	Досліджувані питання	%
	КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА	
1	**Обстановка вчинення кримінального правопорушення**	
	1.1. Місце вчинення протиправних дій	
	1) місця знаходження комп'ютерної техніки, за допомогою якої здійснюються шахрайські дії (стаціонарне комп'ютерне обладнання, ноутбук (телефон, планшет), що переміщується у просторі та підключений до мережі Інтернет)	**29**
	2) місця знаходження банкоматів, банків, у яких знімалася готівка	**18**
	3) місце знаходження потерпілого, який виявив шахрайські дії у процесі здійснення електронних платежів	**22**
	4) інші	**31**
2	**Способи вчинення масових заворушень**	
	2.1. Повноструктурний	**100**
	2.2. Підготовка до вчинення	**100**
	1) підготовка відповідної електронно-обчислювальної техніки	**77**

	(комп’ютер, ноутбук, планшет тощо)	
	2) створення програмного забезпечення для вчинення окремих видів шахрайства	**23**
	3) вибір об’єкта, що буде предметом шахрайських дій	**100**
	4) вибір кола осіб, які стануть жертвами шахрайських дій	**86**
	2.3. Способи безпосереднього вчинення шахрайства у сфері використання банківських електронних платежів	**100**
	1) фішинг	
	2) сніфферінг	
	3) вішинг	
	4) кардинг	
	2.4. Способи приховування	**100**
	1) використання зміни ідентифікатора місця знаходження свого обладнання	**67**
	2) знищення обладнання, яке використовувалось для вчинення кримінальних правопорушень	**73**
	3) надання неправдивих показів під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів	**56**
	4) відмова від дачі показань	**44**
3	**Відомості про слідову картину протиправного діяння**	
	3.1 Матеріальні сліди:	**44**
	1) квитанції та роздруківки про електронні банківські платежі (з банкоматів, телефонів, засобів комп’ютерної техніки тощо)	
	2) банківські картки	
	3) сім-картки	
	4) паперові копії комп’ютерної інформації (копії листування, скріншоти та ін.)	
	5) сліди папілярних ліній на засобах комп’ютерної техніки,	

	клавіатурі терміналу	
	3.2. Електронно-цифрові (віртуальні) сліди:	**100**
	1) у пам’яті мобільного телефону (IMEI-код; історія телефонних з’єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо)	**81**
	2) на сервері мобільного оператора	**25**
	3) на сервері інтернет-провайдера (сервер зберігання flow-статистики и биллінгової інформації, сервер баз даних тощо)	**15**
	4) у пам’яті сім-карти	**78**
	5) у пам’яті комп’ютерів, планшетів	92
	6) у електронній поштовій скриньці	**87**
	7) на флеш карті (файли, папки тощо)	**79**
	8) дані електронного журналу банкомату (терміналу)	**78**
	9) інформація в електронному вигляді, що відображає суми грошових коштів, переказаних через певну систему електронних платежів («Приват-банк», «Qiwi-гаманець», MoneyGram, Western Union, Perfect Money та ін.)	**61**
	10) профіль у соціальних мережах, інформація на сайтах (41 %)	**41**
	3.3. Ідеальні сліди:	**28**
5	**Особа потерпілого**	
	5.1. Віктимогенні групи жертв:	
	1) особи, які піддалися впливу знайомих та родичів під час реалізації банківських електронних платежів	
	2) особи, які піддалися обману незнайомих осіб під час реалізації банківських електронних платежів	
	3) особи, які повідомили свої персональні дані працівникам банківської сфери	
	4) особи, які з огляду на негативні психічні стани піддалися	

	впливу незнайомих осіб під час реалізації банківських електронних платежів	
6	**Дані про особу шахрая**	
	6.1. Стать:	
	1) чоловіча	**79**
	2) жіноча	**21**
	6.2. Вік:	
	1) від 18 до 25 років	**35**
	2) від 25 до 35 років	**44**
	3) від 35 до 45	**17**
	4) особи віком 45 років і старші	**9**
	6.3. Освіта:	
	1) базова середня	**1**
	2) середня	**1**
	3) середня спеціальна	**6**
	4) базова вища	**19**
	5) вища	**73**
	6.4. Сімейний стан:	
	1) у шлюбі	**33**
	2) ні	**67**
	6.5. Рід занять:	
	1) учень (студент)	**17**
	2) працюючий	**80**
	3) працівник сфери підприємницької діяльності та сфери комп'ютерних технологій	**61**
	6.6. Наявність судимості:	**5**
	6.7. Протиправні діяння вчинено у стані сп'яніння:	
	1) алкогольного	**0**
	2) наркотичного	**1**

	6.8. Вчинено ОГ та ЗО:	
	1) так	**23**
	2) ні	**77**
	6.9. Особи, які вчиняють шахрайства у сфері банківських електронних платежів, відрізняються досить високим рівнем інтелекту та посідають авторитетне місце у суспільстві	
	1) так	**71**
	2) ні	**29**
	ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ	
7	**Первинна інформація, що була підставою для внесення даних до ЄРДР за фактом учинення шахрайства у сфері використання банківських електронних платежів, надходили до правоохоронних органів із таких джерел:**	
	1) заяви, листи та повідомлення, що надійшли від громадян, які є потерпілими від визначеного протиправного діяння	**77**
	2) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене правопорушення або стали його свідками	**13**
	3) повідомлення працівників установ, підприємств та організацій	**4**
	4) матеріали слідства, виділені з інших кримінальних проваджень	**1**
	5) матеріали, отримані під час проведення НСРД та розшукових заходів	**5**
8	**Типові слідчі ситуації початкового етапу розслідування шахрайства у сфері використання банківських електронних платежів:**	
	1) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація,	**19**

	шахрай відомий	
	2) вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий	**47**
	3) вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вигляд законних фінансових операцій	**11**
	4) вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація	**23**
	СЛІДЧІ (РОЗШУКОВІ) ДІЇ, НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ДІЇ:	
	Які СРД проводились:	
	1) огляд місця події	**59**
	2) допит потерпілого або представника потерпілої сторони	**100**
	3) огляд ЕОТ, документів	85
	4) освідування	**1**
	5) допит свідка	**14**
	6) допит підозрюваного	**87**
	7) обшук	**58**
	8) призначення судових експертиз	**100**
	9) слідчий експеримент	**6**
	10) пред’явлення особи для впізнання	**5**
	11) одночасний допит раніше допитаних осіб	**18**
9	**Огляд**	
	9.1. Проводився:	**100**
	1) огляд місця події	**59**
	2) огляд місцевості або приміщення, що не є місцем події	**1**

	3) огляд житла чи іншого володіння особи	**2**
	4) огляд предметів	**13**
	5) огляд ЕОТ, документів	**85**
	6) огляд живих осіб (освідування)	**5**
	9.2. Оформлювались додатки до протоколу огляду:	
	1) фототаблиці	**53**
	2) плани и схеми	**31**
	9.3. Помилки, що їх припускаються уповноважені особи під час проведення огляду місця події:	
	1) несвоєчасне проведення огляду	**49**
	2) неаргументоване звуження меж огляду	**83**
	3) непослідовне та поверхневе дослідження на місці події матеріальної доказової інформації	**71**
	4) ігнорування оперативної інформації	**72**
	5) недодержання тактичних рекомендацій щодо деталізованого опису обстановки та об’єктів огляду	**61**
	6) відсутність додатків до протоколу	**41**
10	**Обшук**	
	10.1. Місця проведення:	
	1) зберігання й обробки інформації про банківські електронні платежі, що зазнала злочинного впливу	**67**
	2) знаходження комп’ютерного обладнання, що використовувалося у процесі здійснення протиправного діяння	**43**
	3) збереження інформації, отриманої злочинним шляхом	**41**
	4) настання шкідливих наслідків	**10**
	10.2. Об’єкти обшуку:	
	1) житлові приміщення	**42**
	2) приміщення підприємств, організацій, установ, в т.ч. банків	**37**
	3) підсобні приміщення	**8**

	4) дачі	**5**
	5) транспортні засоби	**4**
	6) гаражі	**1**
	7) інші об’єкти	**3**
11	**Які труднощі виходять із реалізації відомостей НСРД у процесі розслідування шахрайства у сфері банківських електронних платежів:**	
	1) незлагоджена взаємодія підрозділів правоохоронних органів та працівників установ зв’язку	**69**
	2) проблематичність одержання ухвали слідчого судді апеляційного суду стосовно проведення певної НСРД	**61**
	3) відсутність бажання окремих уповноважених осіб покращувати процес кримінального провадження, а також потяг до пошуку легших шляхів для отримання доказової інформації	**32**
	4) брак потреби в огляді та вилученні документів	**48**

Додаток Б

Зведені результати опитувань

25 працівників прокуратури, 317 слідчих, 378 працівників оперативних підрозділів та 62 працівників експертних установ МВС України

	З а п и т а н н я	**%**
1.	**Вкажіть Ваш вік:**	
	До 25 років 25-30 років 31-40 років 41 рік і старше	**23** **32** **37** **8**
2.	**Вкажіть стаж практичної роботи:** до 1 року від 1 до 3 років від 3 до 5 років від 5 до 10 років понад 10 років	 **7** **17** **21** **42** **13**
3.	**Чи розслідували Ви або брали участь у розслідуванні шахрайств:**	
	так	**100**
	ні	**0**
4.	**Чи мали місце у Вашому підрозділі випадки розслідування шахрайства у сфері використання банківських електронних платежів і чи можете Ви надати інформацію з цього приводу:**	
	так	**100**
	ні	**0**
5.	**Чи розслідували Ви особисто або брали участь у розслідуванні шахрайства у сфері використання банківських електронних платежів:**	
	так	**61**
	ні	**39**
6.	**Чи вважаєте Ви, що розслідування кримінальних правопорушень цієї категорії потребує відповідної**	

	кваліфікації уповноваженої особи у зазначеному напрямі:	
	так	**95**
	ні	**5**
7.	**Чи вважаєте Ви одним із найперспективніших напрямів підвищення ефективності розслідування побудову системи сталих кореляційних зв'язків між елементами криміналістичної характеристики шахрайства у сфері банківських електронних платежів:**	
	так	**89**
	ні	**11**
8.	**Чи вважаєте Ви, що обстановку та умови вчинення шахрайства певною мірою визначає вид платіжної системи, через які здійснюються електронні платежі:**	
	так	**67**
	ні	**33**
9.	**Чи вважаєте Ви складання плану розслідування обов'язковим:**	
	так	**86**
	тільки у багатоепізодних справах із великою кількістю підозрюваних	**10**
	ні	**4**
10.	**На Вашу думку, обстановка та умови вчинення шахрайства у сфері електронних банківських платежів визначає й рівень інформаційної безпеки у банківській сфері:**	
	так	**87**
	ні	**13**
11.	**Як Ви вважаєте, чи можливо довести причетність банківських службовців до подібного роду зловживань:**	
	так	**18**
	вкрай важко	**82**
12.	**Вкажіть найбільш характерні позитивні моменти проведення допиту підозрюваного:**	
	дозволяє вчасно висунути слідчі версії	**56**
	дозволяє визначити послідовність проведення інших процесуальних дій	**69**
	дозволяє отримати відомості про особу шахрая	**94**
	дозволяє отримати відомості про обставини протиправного діяння	**39**

	дозволяє з’ясувати дані, що мають тактичне значення	**34**
	дозволяє з’ясувати причини та умови, що сприяли вчиненню шахрайства у сфері використання банківських електронних платежів	**37**
13.	**Чи проводились допити підозрюваних (шахраїв) у конфліктних ситуаціях:**	
	так	**76**
	ні	**24**
14.	**Які тактичні прийоми є найбільш доцільними під час допиту шахрая:**	
	встановлення психологічного контакту	**100**
	викладення показань у формі вільної розповіді	**45**
	актуалізація забутого у пам’яті допитуваного	**61**
	розповідь про ймовірний розвиток події	**21**
	пред’явлення доказів	**93**
	спостереження за поведінкою допитуваного	**75**
15.	**Чи вважаєте Ви, що питання, які стосуються шахрайства у сфері використання банківських електронних платежів, є достатньо складними для сприйняття уповноваженими особами без належної підготовки:**	
	так	**91**
	ні	**9**
16.	**Вкажіть причини, які впливали на те, що у розслідуваних Вами провадженнях не встановлено шахраїв:**	
	недоліки в організації та плануванні розслідування	**45**
	кримінальне правопорушення виявлено через певний проміжок часу	**67**
	знищення окремих слідів та доказів	**69**
	недостатній рівень знань щодо розслідування таких кримінальних правопорушень	**32**
	помилки в оцінці наявної інформації та доказів, унаслідок яких було висунуто та перевірено хибні версії	**19**
	інше	**15**
17	**Вкажіть, які СРД та процесуальні дії проводяться в більшості кримінальних проваджень досліджуваної категорії:**	
	огляд місця події	**38**
	огляд ЕОТ, предметів та документів	**83**
	допит потерпілого	**100**

	допит підозрюваного	**95**
	допит свідків	**21**
	обшук	**59**
	пред'явлення для впізнання	**5**
	слідчий експеримент	**4**
	призначення експертиз	**100**
	тимчасовий доступ до речей та документів	**100**
	інші	**45**
18	**Основні форми використання спеціальних знань** під час **розслідування досліджуваних шахрайств:**	
	консультативно-довідкова допомога	**19**
	участь спеціаліста у проведенні СРД, НСРД	**53**
	призначення експертиз	**100**
	інше	**31**
19	**Вкажіть умови, що сприяють успішному проведенню СРД, НСРД під час розслідування даних кримінальних правопорушень:**	
	всебічна та ретельна підготовка	**100**
	своєчасність у прийнятті рішення	**96**
	правильне застосування тактичних прийомів та їх комплексів	**73**
	використання спеціальних знань, у тому числі інших осіб	**84**
	залучення відповідних спеціалістів	**89**
	інше	**32**
20	**Які чинники, на Вашу думку, впливають на поширення шахрайства у сфері використання банківських електронних платежів? (вкажіть не більше трьох):**	
	недосконалість законодавства у сфері інформаційних відносин	**59**
	недосконалість державного контролю за сферою використання банківських електронних платежів	**63**
	відсутність ефективної взаємодії державних органів між собою	**41**
	віктимна поведінка (недбалість, необізнаність, зайва довірливість тощо) потерпілих	**91**
	високий рівень корумпованості органів державної влади та місцевого самоврядування	**34**
	інше	**27**

Додаток В

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, у яких опубліковано основні наукові результати дисертації:

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

2. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

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

4. 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.

5. Коваленко І. О. Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник.* 2021. № 1 (36). С. 98–101.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

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

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

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

9. Коваленко І. О. До питання криміналістичної характеристики шахрайства в сфері банківських електронних платежів. *Актуальні проблеми експертного забезпечення досудового розслідування*: матеріали наук.-практ. семінару (м. Дніпро, 29 трав. 2020 р.). Дніпро: ДДУВС, 2020. С. 77–79. (доповідь із публікацією тез)

10. Коваленко І. О. Окремі питання визначення обставин, що підлягають встановленню при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Актуальні проблеми криміналістики та судової експертизи*: матеріали наук.-практ. семінару (м. Дніпро, 28 трав. 2021 р.). Дніпро: ДДУВС, 2021. С. 145–147. (доповідь із публікацією тез)

Додаток Г

Акти впровадження результатів дисертаційного дослідження

ЗАТВЕРДЖУЮ
Директор
Дніпропетровського НДЕКЦ МВС
Володимир КОРОТАЄВ
17.04.2020

АКТ

Про впровадження у практичну діяльність Дніпропетровського НДЕКЦ МВС України результатів наукового дослідження Коваленка Іллі Олександровича «Розслідування шахрайства у сфері використання банківських електронних платежів» 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала комісія у складі:

Голови: заступника директора Дніпропетровського НДЕКЦ МВС – завідувача лабораторії криміналістичних видів досліджень П. Кумця

членів комісії: заступника директора Дніпропетровського НДЕКЦ МВС – завідувача лабораторії АД та КДТЗ А. Морохова

заступника завідувача лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС О. Сороки

Комісія відповідно до Положення про організацію проведення НДР і ДКР у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15.05.2007 № 154 склала цей акт з приводу того, що комісією розглянуто результати дисертації аспіранта кафедри криміналістики, судової медицини та психіатрії Дніпропетровського державного університету внутрішніх справ Коваленка Іллі Олександровича «Розслідування шахрайства у сфері використання банківських електронних платежів» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у вигляді наукових статей і тез доповідей на конференціях та семінарах:

Коваленко І.О. Особливості призначення судово-балістичної експертизи // Матеріали Всеукраїнського круглого столу : Сучасні проблеми кримінальної відповідальності, розслідування та запобігання злочинів, вчинених з використанням зброї. (м. Дніпро 14 листопада 2019 р.). Дніпро: Дніпр-й держ. ун-т внутр. справ, 2019. С. 77-80.

Коваленко І.О. До питання протидії шахрайству у сфері використання банківських електронних платежів / І.О. Коваленко, М.М. Єфімов // Матеріали Всеукраїнської науково-практичної конференції : Протидія кіберзагрозам та торгівлі людьми (м. Харків, 26 лист. 2019 р.). Харків : Харківс. нац. ун-т внутр. справ, 2019. С. 169-172.

Коваленко І.О. Деякі аспекти проведення допиту потерпілого при розслідуванні шахрайства у сфері використання банківських електронних платежів // Матеріали Всеукраїнської науково-практичної конференції : Процесуальне та техніко-криміналістичне забезпечення досудового розслідування (м. Харків, 28 лист. 2019 р.). Харків : Харківс. нац. ун-т внутр. справ, 2019. С. 84-66.

Коваленко І.О. Організаційно-практичне забезпечення проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів // Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки). 2019. № 6. С. 130-142.

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 можуть бути впроваджені у діяльність Дніпропетровського НДЕКЦ МВС України.

Голова комісії: **Павло КУМЕЦЬ**

Члени комісії: **Аркадій МОРОХОВ**

Олександр СОРОКА

Затверджую
Начальник УСР
в Дніпропетровській області
ДСР НП України
полковник поліції

Андрій ДАНИЛЯК

«20» 05 2021 року

АКТ

Про впровадження у практичну діяльність управління стратегічних розслідувань в Дніпропетровській області ДСР НП України основних результатів наукового дослідження Коваленка Іллі Олександровича «Розслідування шахрайства у сфері використання банківських електронних платежів» на здобуття освітньо-наукового ступеня доктора філософії за спеціальністю 081 Право

Указала комісія у складі:

Голови: Начальник 9-го відділу УСР
в Дніпропетровській області ДСР НП України
кандидат юридичних наук, майор поліції
Макашов А.В.

Членів комісії: Начальник 10-го відділу УСР
в Дніпропетровській області ДСР НП України
підполковник поліції
Твердоступ І.І.

Старший оперуповноважений 2-го відділу УСР в Дніпропетровській області
ДСР НП України
кандидат юридичних наук
підполковник поліції
Богуславський М.Г.

Комісія відповідно до Положення про організацію проведення НДР і ДКР у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15.05.2007 № 154 склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження

аспіранта кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ Коваленка Іллі Олександровича «Розслідування шахрайства у сфері використання банківських електронних платежів» на здобуття освітньо-наукового ступеня доктора філософії за спеціальністю 081 Право у вигляді наукових статей і тез доповідей на науково-практичних конференціях, семінарах та круглих столах, зокрема:

Коваленко І.О. Організаційно-практичне забезпечення проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2019. № 6. С. 130–142.

Коваленко І.О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

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

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.

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

Коваленко І.О. Особливості призначення судово-балістичної експертизи. *Сучасні проблеми кримінальної відповідальності, розслідування та запобігання злочинів, вчинених з використанням зброї* : матеріали Всеукраїнського круглого столу. (м. Дніпро 14 листопада 2019 р.). Дніпро: Дніпр-й держ. ун-т внутр. справ, 2019. С. 77–80.

Коваленко І.О. До питання протидії шахрайству у сфері використання банківських електронних платежів / І.О. Коваленко, М.М. Єфімов. *Протидія кіберзагрозам та торгівлі людьми* : матеріали Всеукраїнської науково-практичної конференції. (м. Харків, 26 лист. 2019 р.). Харків : Харківс. нац. ун-т внутр. справ, 2019. С. 169–172.

Коваленко І.О. Деякі аспекти проведення допиту потерпілого при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Процесуальне та техніко-криміналістичне забезпечення досудового розслідування* : матеріали Всеукраїнської науково-практичної конференції : (м. Харків, 28 лист. 2019 р.). Харків : Харківс. нац. ун-т внутр. справ, 2019. С. 84–66.

Коваленко И. А. Отдельные аспекты проведения компьютерно-технической экспертизы при расследовании мошенничества в

сфере банковских электронных платежем. *Борьба с преступностью: теория и практики* : материалы VIII Международной научно-практической конференции (г. Могилев, Беларусь, 23 апреля 2020 р.). г. Могилев, Беларусь : Могилевский институт Министерства внутренних дел Республики Беларусь, 2020. С. 483–486.

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

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

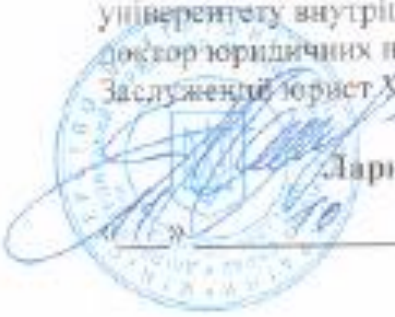
Комісія вважає, що представлені наукові статті та теми доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також можуть бути впроваджені у діяльність управління стратегічних розслідувань в Дніпропетровській області ДСР НП України.

Голова комісії: **Антон МАКАШОВ**

Члени комісії: **Ірина ТВЕРДОСТУП**

Максим БОГУСЛАВСЬКИЙ

ЗАТВЕРДЖУЮ
Проректор
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор,
Заслужений юрист України



Лариса **НАЛИВАЙКО**

«__» _____ 2021 року

АКТ
впровадження в освітній процес
Дніпропетровського державного університету внутрішніх справ
результатів дисертаційного дослідження

11 жовтня 2021 року м. Дніпро

Про впровадження в освітній процес Дніпропетровського державного університету внутрішніх справ основних результатів дисертаційного дослідження Ковалевича Іллі Олександровича «Розслідування шахрайства у сфері використання банківських електронних платежів»

Комісія у складі:

голови: декан факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, доцент Обшалов С.В.

членів комісії: завідувача кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, професора Чаплинського К.О.

професора кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, професора Пирога І.В.

завідувача кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Дарагана В.В.

склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження аспіранта кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ

Коваленка Іллі Олександровича на тему: «Розслідування шахрайства у сфері використання банківських електронних платежів» на здобуття ступеня доктора філософії за спеціальністю 081 Право у вигляді наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

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

Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

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

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.

Коваленко І. О. Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник*. 2021. № 1 (36). С. 98–101.

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

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

Коваленко И. А. Отдельные аспекты проведения компьютернотехнической экспертизы при расследовании мошенничества в сфере банковских электронных платежей. *VIII Международная научно-практическая конференция*. г. Могилев, Республика Беларусь (Могилев, 23 апр. 2020 г.). Могилев : МИМВДРБ, 2020. С. 483–485.

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

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

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

Зазначені наукові статті і тези доповідей внесені до списку літератури робочих програм навчальних дисциплін: «Криміналістика» і «Організація розслідування кримінальних правопорушень» та використовуються під час підготовки курсантів й слухачів до семінарських та практичних занять з зазначених навчальних дисциплін.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та можуть використовуватися в освітньому процесі Дніпропетровського державного університету внутрішніх справ при підготовці фахівців для підрозділів кримінальної поліції, превентивної діяльності, органів досудового розслідування та навчально-наукового інституту заочного навчання та підвищення кваліфікації.

Голова комісії: **Сергій ОБШАЛОВ**

Члени комісії: **Костянтин ЧАПЛИНСЬКИЙ**

Ігор ПИРІГ

Валерій ДАРАГАН

ЗАТВЕРДЖУЮ
Проректор
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор,
Заслужений юрист України

Лариса НАЛИВАЙКО

«18» 10 2021 року

АКТ
впровадження у наукову діяльність
Дніпропетровського державного університету внутрішніх справ
результатів дисертаційного дослідження

19 жовтня 2021 року м. Дніпро

Про впровадження у наукову діяльність Дніпропетровського державного університету внутрішніх справ основних результатів дисертаційного дослідження Коваленка Іллі Олександровича «Розслідування шахрайства у сфері використання банківських електронних платежів»

Комісія у складі:

голови: декан факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, доцент Обшалов С.В.

членів комісії: завідувача кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, доцента Дарагана В.В.

завідувача кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, професора Чаплинського К.О.

професора кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ, доктора юридичних наук, професора Шаблистого В.В.

склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження аспіранта кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ Коваленка Іллі Олександровича на тему: «Розслідування шахрайства у сфері

використання банківських електронних платежів», які використовуються у науково-дослідницькій роботі Дніпропетровського державного університету внутрішніх справ з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень проти власності.

Результати дисертації відображаються у наступних наукових публікаціях:

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

Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

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

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.

Коваленко І. О. Обставини, що підлягають встановленню під час розслідування шахрайства у сфері використання банківських електронних платежів. *Прикарпатський юридичний вісник*. 2021. № 1 (36). С. 98–101.

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

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

Коваленко И. А. Отдельные аспекты проведения компьютерно-технической экспертизы при расследовании мошенничества в сфере банковских электронных платежей. *VIII Международна научно-практическая конференция*. г. Могилев, Республика Беларусь (Могилев, 23 апр. 2020 г.). Могилев : МИМВДРБ, 2020. С. 483–485.

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

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

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

Вказані матеріали дисертаційного дослідження впроваджено у наукову діяльність Дніпропетровського державного університету внутрішніх справ і використовуються з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень проти власності.

Наукові публікації здійснено відповідно до планів науково-дослідницьких робіт Дніпропетровського державного університету внутрішніх справ на 2020-2021 рр. та у межах загальноуніверситетської наукової теми «Актуальні проблеми кримінально-правового, кримінального процесуального та криміналістичного забезпечення протидії злочинності в Україні» (державний реєстраційний номер 0118U100431).

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 відділом організації наукової роботи Дніпропетровського державного університету внутрішніх справ при проведенні наукових досліджень на замовлення Головного Управління Національної поліції в Дніпропетровській області.

Голова комісії: **Сергій ОБШАЛОВ**

Члени комісії: **Валерій ДАРАГАН**

Костянтин ЧАПЛИНСЬКИЙ

Володимир ШАБЛИСТИЙ