МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

КОРШИКОВА ТЕТЯНА ВАСИЛІВНА

УДК 343.985: 343.52 : 004] (072)

ДИСЕРТАЦІЯ

РОЗСЛІДУВАННЯ ШАХРАЙСТВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

081 – Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **Т.В. Коршикова**

Науковий керівник: **Чернявський Сергій Сергійович**, доктор юридичних наук, професор, заслужений діяч науки і техніки України

Київ 2021

АНОТАЦІЯ

Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – Право. – Національна академія внутрішніх справ, Київ, 2021.

Дисертацію присвячено комплексному дослідженню теоретичних, методичних і практичних проблем, пов'язаних з розслідуванням шахрайств, учинених з використанням електронно-обчислювальної техніки.

У розділі 1 «Теоретичні основи та криміналістична характеристика шахрайств, учинених з використанням електронно-обчислювальної техніки» здійснено аналіз стану наукових досліджень проблем розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки (далі – ЕОТ), обґрунтовано позицію, що на сьогодні залишаються недостатньо вивченими в українській криміналістиці питання розслідування кримінальних правопорушень вказаної категорії – монографічні дослідження за цим напрямом не проводились. Це питання було предметом дослідження лише в окремих підрозділах монографій, посібників і методичних рекомендацій, присвячених виявленню та розслідуванню шахрайств або розслідуванню кримінальних правопорушень, вчинених з використанням ЕОТ. Як наслідок, потребують подальшого дослідження способи визначення місцезнаходження ЕОТ, з використанням якої здійснювалось шахрайство, доказування причетності певних осіб до користування такою ЕОТ, вдосконалення проведення окремих слідчих (розшукових) дій під час досудового розслідування кримінальних проваджень вказаної категорії. Виходячи зі стану наукового дослідження проблеми розслідування шахрайств, учинених з використанням ЕОТ, обґрунтовано необхідність здійснення подальших досліджень цієї проблематики.

Надаючи криміналістичну характеристику шахрайств, учинених з використанням ЕОТ, визначено, що предметом шахрайств, учинених за допомогою ЕОТ, можуть бути: майно (рухоме, нерухоме); право на майно; кошти. Останнім часом набуває поширення отримання інформації про банківські картки та установчі дані про особу, яка є власником таких карток.

Констатовано, що дані про спосіб учинення такого кримінального правопорушення є основним підґрунтям для висунення і перевірки слідчих версій щодо особи злочинця та дозволяють встановити слідову картину кримінального правопорушення, оскільки для конкретних способів учинення чи приховання кримінального правопорушення характерні певні види слідів та механізми їх утворення.

За результатами проведеного дослідження встановлено способи вчинення шахрайств з використанням ЕОТ, які умовно поділено залежно від: а) періодичності вчинення кримінального правопорушення; б) сфери застосування; в) кількості задіяних до вчинення шахрайства осіб; г) предмета посягання; д) виду ЕОТ, яка використовувалась; е) інформаційної підтримки; є) характеру «стосунків», що виникають між потерпілим і злочинцем; ж) місця створення та місця реєстрації IP-адреси ЕОТ; з) способів введення в оману або зловживання довірою; і) за характером подання відомостей; ї) використання мережі Інтернет.

Зазначено, що залежно від способів учинення шахрайств з використанням ЕОТ формуються три групи типових слідів: матеріальні (речові), цифрові та віртуальні. Так, до матеріальних можна віднести сліди, що залишаються на ЕОТ та інших засобах, які використовувались під час вчинення шахрайства (на клавіатурі, дисководах, джерелах безперебійного живлення, принтері тощо), а також на предметах, отриманих в результаті шахрайства. До цифрових слідів належать сліди, що вказують на зміни у файловій структурі ЕОТ, а також сліди, яка залишаються в мережі Інтернет під час створення та адміністрування сайтів, облікових записів, сторінок у соціальних мережах, спілкування злочинця з потерпілим, користування

банківськими рахунками. Носіями віртуальних слідів є очевидці кримінального правопорушення, наприклад, особи, які були присутні під час створення сайту, аканту злочинця, використання ЕОТ з протиправною метою чи інших незаконних дій з нею. Місце вчинення кримінального правопорушення обирається з урахуванням можливості реалізації певного способу кримінального правопорушення, предмета посягання, особи жертви. Деякі спроби шахрайства можуть реалізовуватися з кількох місць, не пов'язаних між собою.

З'ясовано, що вивчення особи злочинця є передумовою процесу висунення слідчих версій та планування розслідування, дає змогу обрати найбільш оптимальні тактичні прийоми проведення слідчих (розшукових) дій, а також окреслити коло осіб, які причетні до вчинення цього кримінального правопорушення.

У розділі 2 «Початковий етап розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» визначено типові слідчі ситуації, що можуть виникати під час початкового етапу розслідування вказаних кримінальних правопорушень, які запропоновано поділити на чотири групи залежно від інформації про спосіб вчинення шахрайства та відомостей про особу, яка вчинила такі протиправні дії.

Виокремлено типові загальні версії під час розслідування розглядуваних видів кримінальних правопорушень щодо: а) особи злочинця; б) механізму вчинення шахрайства; в) кількості злочинців; г) кількості вчинених кримінальних правопорушень; д) поширеності шахрайства; е) місця розташування ЕОТ, з якого злочинці вчиняли контакти з потерпілим; є) мотиву вчинення шахрайства. Зроблено висновок, що в основу планування можуть бути покладені як загальні типові, так і окремі версії. Вибір підстав планування залежить від кількості висунутих версій і виявлених епізодів кримінального правопорушення, слідчої ситуації, що склалася, та інших факторів об'єктивного характеру.

Визначаючи основні напрями розслідування шахрайств, учинених з

використанням ЕОТ, вказано на необхідність встановлення місця розташування ЕОТ, з якої здійснювалися дії, або виходу такої ЕОТ в мережу Інтернет, з подальшим встановленням осіб, які користувалися такою ЕОТ під час вчинення кримінального правопорушення.

Підкреслено, що у кримінальному провадженні про вчинення шахрайств з використанням ЕОТ обов'язково потрібно довести факт усвідомлення підозрюваним (обвинуваченим) кримінально-протиправного характеру своїх дій, де винуватість є однією з обставин, які підлягають доказуванню в кримінальному провадженні.

У межах встановлення обставин, що характеризують особу підозрюваного, становить інтерес інформація, яка безпосередньо не пов'язана з учиненим кримінальним правопорушенням (відомості про вік особи, стан її здоров'я, поведінку, колишні судимості тощо). Крім того, до суб'єктивних чинників, що визначають такий структурний елемент криміналістичної характеристики, як «особа злочинця», належать: наявність у злочинців попереднього злочинного досвіду, зокрема й знання конкретних способів учинення, приховування слідів шахрайства, індивідуальні властивості особи злочинця тощо. Підкреслено, що предметом шахрайства, учиненого з використанням ЕОТ, крім майна та права на майно, може бути інформація, зокрема про власників платіжних банківських карток та їх реквізити.

Наведено класифікацію типових слідчих ситуацій на початковому етапі розслідування шахрайств, учинених з використанням ЕОТ. Доведено, що найбільш оптимальним критерієм типізації слідчих ситуацій початкового етапу розслідування вказаних кримінальних правопорушень є обсяг і зміст інформації про спосіб учинення кримінального правопорушення та особу, яка його вчинила. Зазначено, що система типових слідчих версій у кримінальних провадженнях про шахрайство, учинене з використанням ЕОТ, повинна містити два структурних рівні: а) загальні версії як припущення щодо події кримінального правопорушення загалом або окремих елементів

його складу; б) окремі версії, пов'язані з припущеннями щодо інших, більш детальних (допоміжних) обставин учиненого кримінального правопорушення. Визначено основні напрями розслідування шахрайств, учинених з використанням ЕОТ, де основні сили повинні бути сконцентровані на встановленні місця розташування ЕОТ, з якої здійснювалися протиправні дії, з подальшою ідентифікацією особи, яка причетна до такого виду кримінального правопорушення.

У розділі 3. «Проведення окремих слідчих (розшукових) дій та використання спеціальних знань під час розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» зроблено висновок, що найбільш важливими слідчими (розшуковими) діями під час розслідування шахрайств, учинених з використанням ЕОТ, є 1) тимчасовий доступ до інформації, що міститься у провайдерів програмних послуг та Інтернет-провайдерів, з метою встановлення IP-адрес ЕОТ, а також до банків і банківських установ, банківські рахунки яких використовували злочинці; 2) обшук в учасників кримінального правопорушення, проведення якого забезпечує отримання доказової інформації про подію кримінального правопорушення та осіб, які його вчинили, а також 3) безпосередній огляд ЕОТ, яка використовувалась в процесі вчинення шахрайства. Визначено особливості проведення обшуку у досліджуваних кримінальних провадженнях, зокрема: а) необхідність у спеціальних знаннях про структуру та роботу ЕОТ, програмного забезпечення, засобів телекомунікації; б) забезпечення безпечного огляду ЕОТ, отримання відповідних паролів з метою подальшого доступу до інформації, яка знаходиться в ЕОТ; в) дотримання відповідних правил виявлення, вилучення та упакування ЕОТ, інших предметів під час обшуку.

Проведення допитів у кримінальних провадженнях про шахрайства, учинені з використанням ЕОТ, вимагає від слідчих обізнаності у спеціальних питаннях щодо процесу побудови сайтів, створення профілів соціальних мереж, розміщення на них повідомлень і специфіки використання при цьому

відповідного програмного забезпечення та обладнання. Вказане потребує попередньої підготовки до допиту слідчим, що повинна включати: одержання від спеціаліста довідкових даних про місце, час створення сайтів, способів і часу розміщення на них певної інформації, при цьому доцільно запросити на допит спеціаліста, яким чином і звідки здійснювалось адміністрування сайтом, акаунтом; коли були створені електронні скриньки та як вони використовувались у злочинних цілях.

Зазначено, що під час розслідування шахрайств, учинених з використанням ЕОТ, важливою є участь спеціаліста, допомога якого необхідна для: а) застосування науково-технічних засобів і прийомів для виявлення, фіксації та вилучення ЕОТ та інших предметів, за допомогою яких здійснювалися шахрайські дії; б) визначення способу та механізму використання ЕОТ під час вчинення шахрайства; в) пошуку слідів і речових доказів, вилучення слідів, зразків та інших об'єктів, які мають відношення до шахрайства, учиненого з використанням ЕОТ, а також у збереженні вилучених ЕОТ та комп'ютерних програм; г) надання довідкових відомостей, консультації слідчих та інших учасників слідчої (розшукової) дії з приводу застосування спеціальних знань; д) допомоги слідчому щодо правильності викладення виявлених відомостей в протоколі, а також у складанні схем, планів місця розташування і підключення ЕОТ та інших предметів; е) формулювання питань особам, яких будуть допитувати у зв'язку з їх перебуванням на місці кримінального правопорушення.

Водночас у процесі розслідування шахрайств, учинених з використанням ЕОТ, проводяться наступні види експертиз, які забезпечують повне та всебічне розслідування цих кримінальних правопорушень: 1) експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза); 2) дактилоскопічна експертиза відбитків слідів рук осіб, які були вилучені з ЕОТ та інших предметів, а також у приміщенні, де здійснювалось використання ЕОТ з метою вчинення шахрайства; 3) експертиза матеріалів і засобів звукозапису, де об'єктом дослідження

можуть бути записи дій та переговори осіб, причетних до шахрайства; 4) молекулярно-генетична експертиза з метою дослідження біологічних зразків, відібраних у живих осіб, і слідів біологічного походження, вилучені під час проведення слідчих (розшукових) дій.

Залежно від способів вчинення шахрайства можуть назначатись й інші види експертиз, експертизи матеріалів документів, експертизи документів бухгалтерського, податкового обліку і звітності, технічна експертиза документів тощо. Щодо особи, то тут, як правило, назначається судово-психіатрична експертиза підозрюваного і проводиться вона тоді, коли відносно нього виникає сумнів в його психічній повноцінності.

Ключові слова: шахрайство, електронно-обчислювальна техніка, слідчі (розшукові) дії, розслідування, комп'ютерні технології, початковий етап розслідування, слідчі (розшукові) дії, кримінальне провадження.

ANNOTATION

Korshykova T. V. Investigation of fraud committed with the use of computer technology.– Qualifying scientific work on the rights of the manuscript.

The dissertation on a scientific degree competition for the candidate of legal sciences on a specialty 081 – «Law». – National Academy of Internal Affairs, Kyiv, 2021.

The dissertation is devoted to a comprehensive study of theoretical, methodological and practical problems associated with the investigation of fraud committed with the use of computer technology.

In the first section "Theoretical foundations and forensic characteristics of fraud committed with the use of computer technology", carrying out the analysis of a scientific researches condition of the investigation problems of the frauds made with use of computer technology, it is substantiated, that the issues of investigation of this category of criminal offenses remain insufficiently studied in Ukrainian criminology. Monographic studies in this area have not been conducted yet. This issue has been the subject of research, but only as a part of sections in different monographs, manuals and guidelines for the fraud detection and investigation or for the investigation of criminal offenses committed using computer technology. As a result, we can talk about necessity of the further research on the methods of determining the location of the electronic computing basis, using which fraud was carried out; proving the involvement of certain persons in the use of such computer technology; improving certain investigative (search) actions during the pre-trial investigation of criminal proceedings. Based on the state of scientific research on the problem of investigating fraud committed with the use of computer technology, the need for further research on this issue is justified.

Giving a forensic description of fraud committed with the use of electronic computing, it is determined that the subject of fraud committed with its help can be: property (movable, non-movable); right to property; money funds. Recently, information about bank cards and constituent data about the person, who owns such cards, has become widespread. It is stated that data on the manner of

committing such a criminal offense is the main basis for proposing and verifying investigative versions about the offender. Said data allows define traces of the criminal offense, as specific ways of committing or concealing a criminal offense are characterized by certain types of traces and mechanisms.

According to the results of the study, the methods of committing fraud using electronic computing were defined and conditionally divided depending on: a) the frequency of the commission of a criminal offense; b) areas of application; c) number of persons involved in committing fraud; d) subject of encroachment; e) type of computer technology used; f) information support; g) nature of the "relationship" that arises between the victim and the offender; g) place of creation and place of registration of the IP address; h) ways to mislead or abuse trust; i) nature of the information submission; j) use of the Internet.

It is noted that depending on the methods of committing fraud using computer technology, three groups of typical traces are formed: material (real), digital and virtual. Thus, the material traces can be left on the computer technologies and other tools used during the fraud (on the keyboard, disk drives, uninterruptible power supplies, printers, etc.), as well as on items obtained as a result of fraud. Digital traces include ones that indicate changes in the file structure of the computer, as well as traces that remain on the Internet during the creation and administration of sites, accounts, pages on social networks, communication between the offender and the victim, or bank accounts usage. Carriers of virtual traces are eyewitnesses of a criminal offense, for example, persons who were present during the creation of the site, the criminal's acanthus, or usage of computer technology for illegal purposes or actions.

The place where criminal offense has been committed is chosen taking into account the possibility of implementing the chosen method of criminal offense, the subject of encroachment, the identity of the victim. Some fraud attempts can be made from several unrelated locations. It was found that the study of the identity of the offender is a prerequisite for the process of proposing investigative versions

and planning the investigation. It allows you to choose the most optimal tactics of investigative (search) actions, as well as outline the persons involved in this crime.

In the second section "Initial stage of investigation of fraud committed with the use of computer technology" typical investigative situations that may arise during the initial stage of the investigation of criminal offenses are identified. Such decisions are proposed to be divided into four groups depending on the information about the method of committing fraud and information about the person who committed such illegal acts.

Typical versions arising during the investigation of the considered types of criminal offenses are related to: a) the person of the criminal; b) the mechanism of committing fraud; c) the number of criminals; d) the number of committed criminal offenses; e) the prevalence of fraud; f) the location of the computer technology from which the perpetrators made contact with the victim; g) the motive for committing fraud. It is concluded that the planning can be based on both standard and individual deductive versions. The choice of grounds for planning depends on the number of advanced versions and the identified episodes of the criminal offense, the current investigative situation and other objective factors.

The main directions for investigation of fraud committed with the use of computer technologies ere defined. The need to establish the location of computers, from which illegal actions were carried out, or access of such computers to the Internet, followed by identification of persons, who used such computer technologies during the commission of a criminal offense, was emphasized.

It is emphasized that in criminal proceedings on committing fraud with the use of computer technologies it is necessary to prove the fact that the suspects are aware of the criminally illegal nature of their actions, where guilt is one of the circumstances to be proved in criminal proceedings.

Within the framework of establishing the circumstances that characterize the suspect's identity, information that is not directly related to the committed criminal

offense (information about the age of the person, his state of health, his behavior, previous convictions, etc.) is one of great interest. In addition, the subjective factors that determine such a structural element of forensic characteristics as "criminal identity" include: the presence of previous criminal experience, including knowledge of specific methods of committing fraud and concealment of any traces, individual characteristics of the offender, and so on. It is emphasized that information, in particular about the holders of payment bank cards and their details, may be the subject of fraud, committed with the use of computer technologies, in addition to property and property rights.

The classification of typical investigative situations at the initial stage of investigation of fraud committed with the use of computer technologies is given. It is proved that the most optimal criterion for typification of investigative situations for the initial stage of criminal offenses investigation is the amount and content of information about the method of committing a criminal offense and the person, who committed it. It is noted that the system of standard investigative versions in criminal proceedings on fraud committed with the use of computer technologies should contain two structural levels: a) general versions as assumptions about the event of a criminal offense in general or individual elements of its composition; b) separate versions related to assumptions about other, more detailed circumstances of the committed criminal offense. The main directions of investigation of fraud committed with the use of computer technologies, where the main forces should be concentrated on establishing the location of computer technologies, which the illegal actions were carried out from, with subsequent identification of the person involved in this type of criminal offense, were determined.

The third section "Carrying out certain investigative (search) actions and use of special knowledge during the investigation of fraud committed with the use of computer technologies" concludes that the most important investigative (investigative) actions in the investigation of computer technologies fraud are: 1) temporary access to information contained in software service providers and

Internet providers, as well as to banks and banking institutions whose bank accounts were used by criminals, in order to establish the IP addresses of computer technologies; 2) search for the participants of the criminal offense, the conduct of which ensures the receipt of evidentiary information about the criminal offense and the persons who committed it, 3) direct inspection of the computer technologies, which were used in the process of committing fraud. The peculiarities of the investigating search actions in the investigated criminal proceedings are determined, in particular: a) the need for special knowledge about the structure and operation of computer technologies, software, telecommunications; b) ensuring a secure inspection of the computer technologies, obtaining appropriate passwords for further access to information contained in the computer technologies; c) compliance with the relevant rules for the detection, removal and packaging of computer technologies and other items during the search.

Interrogation in criminal proceedings on fraud committed with the use of computer technologies requires investigators to be aware of special issues related to the process of building sites, creating profiles of social networks, posting messages on them and the specifics of using the appropriate software and hardware. This requires prior preparation for questioning by investigators, which should include: obtaining reference data on the place, time of creation of sites, methods and time of placing certain information from the specialist (it is advisable to invite the specialist for questioning on how and where the administration of the site or account located); when e-mail boxes were created and how they were used for criminal purposes.

It is noted that in the investigation of fraud committed with the use of computer technologies, it is important to involve a specialist, whose help is needed to: a) use scientific and technical tools and methods for the detection, fixation and seizure of computer technologies and other items by which fraudulent acts were carried out; b) determine the method and mechanism of use of computer technologies during fraud process; c) search for traces and physical evidence, removal of traces, samples and other objects related to fraud committed with the

use of computer technologies, as well as in the preservation of computer technologies and computer programs that have been seized; d) provide background information, consulting investigators and other participants in the investigative (search) action on the application of special knowledge; e) assist the investigator in the correct presentation and protocoling of the information found; to draw up diagrams, location plans and connection of computer technologies and other items; f) formulate questions for persons who will be interrogated in connection with their location at the scene of a criminal offense.

At the same time, in the process of investigating fraud, committed with the use of computer technologies, the following types of examinations, to provide a full and comprehensive investigation of these criminal offenses, are conducted: 1) examination of computer equipment and software products (computer technical examination); 2) dactyloscopic examination of fingerprints of persons, removed from the computer technologies and other objects, or taken around the rooms where the use of computer technologies was carried out for the purpose of committing fraud; 3) examination of materials and tools of sound recording, where the object of research may be recordings of actions and negotiations between persons involved in fraud; 4) molecular genetic tests for the purpose of the search for biological samples taken from living persons and traces of biological origin, taken during investigative (search) activities.

Depending on the methods of committing fraud, other types of examinations, examination of document materials, examination of accounting documents, tax accounting and reporting, technical examination of documents, etc. may be appointed. As for the person, a forensic psychiatric examination of the suspect is usually appointed and carried out when there are doubts about the mental integrity of the suspect.

Key words: fraud, computer technology, investigative (search) actions, investigations, computer technologies, initial stage of investigation, investigative (search) activities, criminal proceedings.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

праці, в яких опубліковано основні наукові результати дисертації:

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

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

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

4. Романенко (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.

5. Романенко (Коршикова) Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. P. 129–135. (Словацька Республіка).

праці, які засвідчують апробацію матеріалів дисертації:

6. Романенко (Коршикова) Т. В. Алгоритм дій слідчого з розслідування шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні питання криміналістики*: матеріали Всеукр. наук.-практ. конф. (Київ, 20 груд. 2019 р.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ: Нац. акад. внутр. справ, 2019. С. 368–370.

7. Романенко (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.

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

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

які додатково відображають наукові результати дисертації

10. Тарасенко О. С., Федоренко О. А., Стрільців О. М. та ін. Пошук кримінально значимої інформації в мережі Інтернет: метод. рек. / за ред. Ю. Ю. Орлова. К.: Нац. акад. внутр. справ, 2020. 100 с.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДНДЕКЦ	Державний науково-дослідний експертно-криміналістичний центр
ЄДРСР	Єдиний державний реєстр судових рішень
ЄРДР	Єдиний реєстр досудових розслідувань
ЕОТ	електронно-обчислювальна техніка
КПК	Кримінальний процесуальний кодекс
МВС	Міністерство внутрішніх справ
НП	Національна поліція
НСРД	негласні слідчі (розшукові) дії
ПВСУ	Пленум Верховного Суду України
СОГ	слідча оперативна група
СРД	слідча (розшукова) дія

ВСТУП

Обґрунтування вибору теми дослідження. Можливості електронно-обчислювальної техніки та Всесвітньої мережі Інтернет безмежні, а їх використання відіграє все більшу роль у політичних, економічних і соціальних процесах в Україні та світі. Близько 78 % населення України віком 16 років і старше (приблизно 25 млн осіб) користується Інтернетом, при цьому покупки через Інтернет здійснюють понад 11 млн українців, з них кожний четвертий робить понад 20 замовлень на рік. Поряд з цим зростають негативні тенденції у суспільстві, відбуваються якісні та кількісні зміни кіберзлочинності, яка набуває все більш професійного, організованого та витонченого характеру. Через велику популярність онлайн-шопінгу збільшилася й активність онлайн-шахраїв. За статистикою ресурсу OLX Україна, частка шахрайств лише в онлайн-шопінгу з використанням сайтів-підробок становить близько 0,4 % від усіх транзакцій, а за даними Української міжбанківської асоціації членів платіжних систем ЄМА[1], за допомогою Інтернет-мережі шахраї «заробили» 252 млн грн. Як наслідок, лише у 2020 р. до підрозділів кіберполіції Національної поліції України надійшло понад 33 тис. звернень (повідомлень) громадян стосовно шахрайський дій щодо них, вчинених у мережі Інтернет[2]. Найбільш розповсюдженими схемами вчинення шахрайств були продаж неіснуючих товарів на платформах оголошень або у соціальних мережах, а також використання фішингових ресурсів, які ззовні схожі на популярні інтернет-магазини, банківські установи або організації. Також у 2020 р. набули популярності шахрайські схеми, замасковані під сервіси доставки платформ оголошень.

Вказане ставить перед наукою завдання, спрямовані на розробку новітніх прийомів, методів і засобів розслідування шахрайств, вчинених з

[1] Української міжбанківської асоціація членів платіжних систем ЄМА. *Офіційний вебсайт.* URL: https://www.ema.com.ua/

[2] Кіберполіція України. *Офіційний вебсайт.* URL: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/

використанням ЕОТ.

Досвід розслідування шахрайств, учинених з використанням ЕОТ, свідчить про недостатню ефективність наявних засобів і методів розслідування таких кримінальних правопорушень. Така ситуація обумовлена багатьма чинниками, серед яких головними є відсутність достатніх знань під час проведення слідчих (розшукових) дій, зокрема пов'язаних з оглядом ЕОТ; недотримання слідчими рекомендацій щодо тактики проведення окремих слідчих (розшукових) дій та призначення експертиз; неналежна взаємодія слідчих з оперативними та експертними підрозділами тощо. Як наслідок, відсутність методики розслідування шахрайств, учинених з використанням ЕОТ, негативно впливає на результати правоохоронної діяльності в даному напрямі. У цьому контексті важливим є узагальнення наукових ідей і підходів до створення якісно нового механізму розслідування вказаних кримінальних правопорушень.

Теоретичним підґрунтям дисертаційного дослідження стали праці вітчизняних й іноземних учених, які приділяли значну увагу теоретичним і практичним засадам криміналістичного дослідження розслідування кримінальних правопорушень, що вчиняються в сфері інформаційних технологій та з використанням ЕОТ, серед яких: Д. С. Азаров, Б. В. Андрєєв, Р. С. Атаманов, О. А. Баранов, В. М. Бутузов, Т. В. Варфоломеєва, М. С. Вертузаєв, В. Д. Гавловський, В. О. Голубєв, В. Г. Гончаренко, В. А. Губанов, М. В. Гуцалюк, В. Г. Дрозд, Д. О. Зиков, М. І. Камлик, М. В. Карчевський, В. А. Колесник, А. А. Комаров, О. І. Котляревський, В. В. Крилов, О. В. Лисодєд, В. Б. Міщенко, О. І. Мотлях, В. І. Оборський, Л. П. Паламарчук, І. В. Рогатюк, Б. В. Романюк, С. В. Самойлов, О. В. Смаглюк, О. М. Стрільців, О. І. Усов, В. П. Хорст, В. С. Цимбалюк, Ю. М. Чорноус, В. П. Шеломенцев, О. М. Юрченко та інші.

Що стосується шахрайств, то основи методик розслідування зазначеного кримінального правопорушення були закладені такими науковцями, як А. І. Анапольська, С. В. Головкін, С. М. Князєв,

Н. Ю. Кириленко, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, С. С. Чернявський та інші.

Разом з тим варто відмітити, що хоча результати проведених досліджень були спрямовані на удосконалення розслідування шахрайства, учиненого з використанням ЕОТ, проте опубліковані роботи не вирішили всіх проблем організаційного та тактичного характеру, які виникають при розслідування таких кримінальних правопорушень, що спонукає до необхідності проведення комплексного наукового дослідження розслідування шахрайства, учиненого з використанням ЕОТ, що визначає актуальність обраної теми дослідження, її наукову, теоретичну та практичну значущість.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 р., затвердженого Постановою Кабінету Міністрів України від 7 вересня 2011 р. № 942; Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 р., затвердженої розпорядженням Кабінету Міністрів України від 15 листопада 2017 р. № 1023-р, та Плану заходів з її реалізації, затвердженого розпорядженням Кабінету Міністрів України від 21 серпня 2019 р. № 693-р; п. 14, 15, 27 Тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки, затвердженої наказом Міністерства внутрішніх справ України від 11 червня 2020 р. № 454; Пріоритетних напрямів наукових досліджень Національної академії внутрішніх справ на 2018–2020 рр. (рішення Вченої ради від 26 грудня 2017 р., протокол № 28). Тему дисертації затверджено рішенням Вченої ради Національної академії внутрішніх справ від 18 листопада 2017 р. (протокол № 27) та включено до Переліку тем дисертаційних досліджень з проблем держави і права Національної академії правових наук України (за № 1135/2017).

Мета і завдання дослідження. *Метою* роботи є комплексне

дослідження теоретичних, методичних і практичних рекомендацій, що спрямовані на удосконалення організації й тактики розслідування шахрайств, учинених з використанням ЕОТ.

Реалізація зазначеної мети обумовила постановку та вирішення таких *завдань:*

– визначити стан наукових досліджень проблем розслідування шахрайств, учинених з використанням ЕОТ;

– визначити предмет злочинного посягання та способи шахрайств, учинених з використанням ЕОТ;

– розкрити слідову картину та обстановку вчинення шахрайств, учинених з використанням ЕОТ;

– надати характеристику особи злочинця та особи потерпілого від шахрайств, учинених з використанням ЕОТ;

– окреслити обставини, що підлягають встановленню під час розслідування шахрайств, учинених з використанням ЕОТ;

– виокремити типові слідчі ситуації та слідчі версії, що виникають під час розслідування шахрайств, учинених з використанням ЕОТ;

– визначити основні напрями розслідування шахрайств, учинених з використанням ЕОТ;

– узагальнити особливості проведення вербальних слідчих (розшукових) дій під час розслідування шахрайств, учинених з використанням ЕОТ;

– узагальнити особливості проведення невербальних слідчих (розшукових) дій під час розслідування шахрайств, учинених з використанням ЕОТ;

– розкрити особливості використання спеціальних знань під час розслідування шахрайств, учинених з використанням ЕОТ.

Об’єкт дослідження – суспільні відносини, що виникають під час розслідування шахрайств, учинених з використанням ЕОТ.

Предмет дослідження – розслідування шахрайств, учинених з використанням ЕОТ.

Методи дослідження. Методологічним підґрунтям наукового дослідження є *діалектичний метод пізнання* соціально-правових явищ, використання якого надає можливість детально проаналізувати об'єкт, предмет, мету та завдання дисертації (розділи 1–3). Для виконання поставлених завдань і досягнення мети було використано комплекс загальнонаукових і спеціальних методів наукового пізнання, зокрема: *гносеологічний* – для окреслення поглядів учених щодо проблем розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки (підрозділ 1.1); *порівняльно-правовий* – для аналізу поглядів науковців щодо досліджуваної проблематики, наукових категорій, визначень і підходів (розділи 1–3); *системний* – для здійснення класифікації способів учинення кримінальних правопорушень (підрозділ 1.2); *типологічний* – у процесі формування характеристики особи злочинця (підрозділ 1.4); *методи аналізу* і *синтезу* – під час формування висновків з питань, які висвітлюються в дисертації; *структурно-функціональний* – для визначення функціональної спрямованості результатів дослідження шахрайств, учинених з використанням ЕОТ (розділи 1–3); *статистичний* – у процесі проведення аналізу та узагальнення емпіричної бази (вивчення кримінальних проваджень, відомостей Єдиного державного реєстру судових рішень, результатів анкетування) (розділи 1–3); *соціологічний* для підтвердження наукових висновків результатами анкетування та інтерв'ювання працівників підрозділів Національної поліції (розділи 1–3).

Емпіричну базу дослідження становлять результати узагальнення експертної, слідчої та судової практики, зведені результати опитування 300 слідчих Національної поліції з усіх регіонів держави за напрямом дослідження, узагальнені результати вивчення матеріалів 40 кримінальних проваджень. Використано також власний досвід роботи дисертанта у слідчих підрозділах Національної поліції України.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших в Україні комплексних досліджень теоретичних і практичних проблем розслідування шахрайств, учинених з використанням ЕОТ, у якому сформульовано низку нових наукових положень, висновків та рекомендацій, зокрема:

вперше:

– розроблено алгоритм першочергових заходів, які здійснюють уповноважені підрозділи Національної поліції України в разі надходження інформації про шахрайство, вчинене з використанням ЕОТ, які об'єднано в блоки: з'ясування обставин шахрайства; внесення відомостей до ЄРДР; визначення напрямів встановлення IP-адрес, які використовувались ЕОТ з метою вчинення шахрайства; виявлення ЕОТ, які використовувались з метою вчинення шахрайства; фіксація причетності осіб до використання ЕОТ з метою вчинення шахрайства та отримання/неотримання коштів чи майна під час вчинення шахрайства; проведення СРД та НСРД;

– визначено обставини, які підлягають встановленню під час розслідування шахрайств, учинених з використанням ЕОТ;

– розроблено наукові основи розслідування шахрайства, вчиненого з використанням ЕОТ, а також структуру криміналістичної характеристики, до якої включено такі елементи: предмет злочинного посягання та спосіб вчинення кримінального правопорушення, у поєднанні зі способами готування і приховування вчинення шахрайства з використанням ЕОТ; слідова картина вчиненого кримінального правопорушення, типові цифрові сліди такого виду шахрайства та механізм їх утворення; особа злочинця та особа потерпілого; обстановку вчинення – місце, час, умови та інші обставини, що є типовими для вчинення кримінального правопорушення цієї категорії;

– визначено порядок і тактику огляду ЕОТ, а також інформації, що міститься в ній, з метою виявлення матеріальних та цифрових слідів, які можуть бути доказами у кримінальних провадженнях про вчинення

шахрайства з використанням ЕОТ;

удосконалено:

– криміналістичні рекомендації щодо проведення окремих слідчих (розшукових) дій, спрямованих на встановлення осіб, причетних до шахрайств, учинених з використанням ЕОТ;

– характеристику осіб, які можуть бути причетні до вчинення шахрайств з використанням ЕОТ;

– наукові положення щодо використання спеціальних знань під час розслідування шахрайств, учинених з використанням ЕОТ, залучення спеціалістів для надання допомоги під час проведення слідчих (розшукових) дій та надання консультацій спеціалістами;

дістали подальший розвиток:

– теоретичні положення щодо участі спеціаліста в підготовці та проведенні окремих слідчих (розшукових) дій під час розслідування шахрайств, учинених з використанням ЕОТ;

– характеристика типових слідчих ситуацій початкового етапу розслідування шахрайств, учинених з використанням ЕОТ;

– положення про способи шахрайств, учинених з використанням ЕОТ, залежно від об’єкта та предмета посягання, використання Інтернет-мережі;

– напрями розслідування шахрайств, учинених з використанням ЕОТ, залежно від слідчої ситуації, що склалася на початковому етапі;

– організаційно-тактичні основи проведення обшуку та допиту підозрюваних як засобів збирання доказів під час розслідування шахрайств, учинених з використанням ЕОТ.

Практичне значення отриманих результатів полягає в тому, що сформульовані та викладені в дисертації теоретичні положення, висновки, пропозиції і рекомендації впроваджено та надалі може бути використано у:

– *практичній діяльності слідчих підрозділів Національної поліції* – для вдосконалення розслідування шахрайств, учинених з використанням ЕОТ (акт впровадження Головного слідчого управління Національної поліції

України від 28 січня 2021 р.);

– освітньому процесі Національної академії внутрішніх справ – у системі професійної освіти слідчих, підвищенні кваліфікації поліцейських, при викладанні відповідних навчальних дисциплін і підготовці навчальних і методичних посібників, підручників, курсів лекцій (акт впровадження Національної академії внутрішніх справ від 21 січня 2021 р.).

Особистий внесок здобувача. Положення, що викладені в дисертації та виносяться на захист, розроблені автором особисто. Наукові ідеї та розробки, що належать співавторам опублікованих робіт, у дисертації не використовуються. У методичних рекомендаціях «Пошук кримінально значимої інформації в мережі Інтернет» особистий внесок дисертанта становить 10 %. У статті в співавторстві з О. В. Бишевець особистий внесок здобувача становить 50 %.

Апробація матеріалів дисертації. Основні положення, висновки та результати дослідження оприлюднені автором у виступах на всеукраїнських та міжнародних науково-теоретичних і науково-практичних конференціях, засіданнях круглих столів, зокрема: «Актуальні питання криміналістики» (м. Київ, 20 грудня 2019 р.), «Актуальні проблеми кримінального права» (м. Київ, 20 листопада 2020 р.), «Кримінальний процес та криміналістика: сучасний стан та перспективи» (м. Харків, 26 листопада 2020 р.), «Актуальні проблеми кримінального права, процесу та криміналістики та оперативно-розшукової діяльності» (м. Хмельницький, 26 лютого 2021 р.).

Публікації. Основні положення та висновки, що сформульовані в дисертації, відображено у 10 наукових публікаціях, серед яких чотири статті у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук; одна стаття – у міжнародному юридичному виданні, чотири тези доповідей, опублікованих у збірниках матеріалів науково-практичних конференцій, а також одні методичні рекомендації.

Структура та обсяг дисертації. Дисертація складається з анотації, переліку умовних позначень, вступу, трьох розділів, що містять десять

підрозділів, висновків, списку використаних джерел (266 найменування на 29 сторінках), чотирьох додатків (на 13 сторінках). Загальний обсяг дисертації становить 255 сторінок, з яких основний текст дисертації становить 197 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ТА КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ШАХРАЙСТВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

1.1 Стан наукових досліджень проблем розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки

Поняття «шахрайство» наразі закріплено в ст. 190 КК України, ч. 1 якої визначає його як заволодіння чужим майном або придбавання права на майно, шляхом обману чи зловживання довірою [131]. Крім цього, ч. 2–4 вказаної статті передбачають низку кваліфікуючих ознак шахрайства, серед яких ч. 3 визначає «вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки».

Наявність зазначеної кваліфікуючої ознаки є цілком виправданою, відповідає сучасному етапу розвитку суспільства й науково-технічного прогресу та необхідності посилення уваги до питань протидії злочинності у сфері комп'ютерної інформації («комп'ютерні» кримінальні правопорушення), про що неодноразово зазначають у своїх дослідженнях низка науковців [10, с. 191]. До того ж на «шахрайство, пов'язане з комп'ютерами (комп'ютерне шахрайство)» звертає увагу й ратифікована Україною Конвенція про кіберзлочинність від 23 листопада 2001 р. Зокрема, зі змісту ст. 8 цієї Конвенції випливає, що шахрайство, пов'язане з комп'ютерами, – це навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: a) будь-якого введення, зміни, знищення чи приховування комп'ютерних даних; b) будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи [109].

Поняття «комп'ютерне шахрайство» з'явилося ще в 70-і рр. минулого

століття, коли в розвинених країнах підвищився рівень економічних кримінальних правопорушень [5], що спричинило потребу реформування законодавства, але законодавчі органи були деякою мірою розгублені, адже на перший погляд могло б здатися, що можна тільки об'єднати низку кваліфікуючих ознак і чинних норм законодавства, та при уважнішому розборі конструкції таких кримінальних правопорушень видно, що тут з'являється можливість говорити про появу нового способу та нового предмета посягань, що призвело до необхідності введення нових складів у КК України [131], які містять відповідальність за такі види кримінальних правопорушень.

Це, своєю чергою, спричинило плюралізм наукових позицій щодо трактування дефініцій «електронно-обчислювальна техніка», «комп'ютер», «кіберзлочинність» та ін. Якщо звернутися до позицій науковців у галузі кримінального права, то конструкція «шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки», на думку Л. М. Кривоченка, свідчить про специфічний спосіб вчинення цього кримінального правопорушення, при цьому його небезпечність полягає в тому, що ця техніка значно полегшує вчинення шахрайства, дозволяє заволодівати значними коштами, завдаючи непоправної шкоди власникам [130, с. 160], а М. І. Хавронюк вважає, що ЕОТ у ч. 3 ст. 190 КК України є засобом вчинення шахрайства [243, с. 196].

Проте, М. І. Мельник найбільш змістовно визначає, що: по-перше, зміст цієї ознаки полягає у спрямованій на заволодіння чужим майном або придбання права на майно операції, в основі якої лежать обман чи зловживання довірою (при цьому вказану ознаку утворюють лише операції, здійснення яких без використання ЕОТ є неможливим, наприклад, здійснення електронних платежів, інших операцій з безготівковими коштами); по-друге, якщо з використанням такої техніки здійснюються операції, які цілком можуть здійснюватися за допомогою іншої техніки (наприклад, комп'ютер використовується для набору тексту, виготовлення документа тощо), то

розглядуваний склад шахрайства відсутній [12, с. 197].

Великий тлумачний словник сучасної української мови визначає поняття «електронно-обчислювальна», як виконана із застосуванням електроніки, а «обчислювальну техніку», як галузь техніки, що поєднує в собі теоретичні основи та практичні аспекти обчислювальних машин [41]. Окрім цього, словник дає визначення «електронно-обчислювальна машина», що тлумачиться як цифрова обчислювальна машина, основні вузли якої реалізовані засобами електроніки [41]. Також в словнику зустрічається поняття «персональна обчислювальна машина», яке визначається як ЕОМ, призначена для обслуговування одного користувача, що характеризується невеликими габаритами; персональний комп'ютер [41]. Також словник визначає поняття «комп'ютер», як електронно-обчислювальна машина (ЕОМ). Тобто, поняття комп'ютер та ЕОМ є тотожними.

Проаналізувавши визначення, ми доходимо висновку, що «електронно-обчислювальна техніка» є ширшим поняттям і включає в себе ЕОМ (комп'ютери), системи пристроїв, обладнання до них та інші види електронно-обчислювальних пристроїв (мобільні телефони, планшети та інші електроприлади, де для вчинення шахрайства використовується їх програмне забезпечення, а не аудіодзвінок).

Складовими ЕОТ є:

– материнська плата;

– процесор;

– пристрої пам'яті;

– пристрої введення;

– пристрої виведення

– наявність програмного забезпечення [228, с. 45–48].

Своєю чергою, кваліфікувати ЕОТ можна за різними параметрами:

а) за автономністю (мобільністю) живлення:

– стаціонарні (системні) пристрої;

– мобільні пристрої;

б) за доступом:

– здійснюється безпосередній доступ до ЕОТ;

– здійснюється віддалений (опосередкований) доступ до ЕОТ;

в) за належністю пристрою:

– побутове;

– спеціально придбане (налаштоване);

г) за доступом до Інтернет-мережі:

– присутній доступ;

– доступ відсутній;

д) за кількістю залучених до вчинення шахрайств ЕОТ:

– одна ЕОТ;

– дві і більше ЕОТ, які можна встановити;

– не визначена кількість ЕОТ;

е) за наявністю програмного забезпечення:

– встановлено стандартне (базове) програмне забезпечення;

– встановлено спеціальне обладнання з метою вчинення шахрайства.

Нині шахрайство з використанням ЕОТ зберігає сталу тенденцію до еволюціонування, з'являються нові його види чи удосконалюються вже відомі, такі як: у сфері дистанційного банківського обслуговування, з електронними платіжними системами і системами експрес-оплати товарів і послуг (жебрацтво, фейкові банки, біржі праці, електронні віртуальні гаманці, фейкові листи від чужого імені, інтернет-аукціони, інтернет-лотереї, віртуальні казино й тоталізатори), кредитне шахрайство, кіберсквоттинг, рерайтинг, серфінг, креммінг, банкоматне шахрайство (фішинг, скіммінг, використання «білого пластику»), використання шпигунських програм (spyware, keyloggers), використання ноах-програмного забезпечення, SMS-шахрайство тощо [256, с. 145].

Тому науковці активно розробляють питання, пов'язані з методикою розслідування кримінальних правопорушень, учинених з використанням ЕОТ, зокрема, Д. С. Азаров, Б. В. Андрєєв, О. А. Баранов, Ю. М. Батурін,

В. М. Бутузов, Т. В. Варфоломеєв, М. С. Вертузаєв, О. Г. Волєводз, В. Д. Гавловський, В. О. Голубєв, В. Г. Гончаренко, В. А. Губанов, М. В. Гуцалюк, Д. О. Зиков, М. І. Камлик, М. В. Карчевський, В. А. Колесник, А. А. Комаров, О. І. Котляревський, В. В. Крилов, В. Д. Ларичев, А. К. Лебедєв, О. В. Лисодєд, В. Б. Міщенко, О. І. Мотлях, В. І. Оборський, Б. В. Романюк, О. В. Смаглюк, О. М. Стрільців, О. І. Усов, С. С. Чернявський, В. П. Хорст, В. С. Цимбалюк, В. П. Шеломенцев, О. М. Юрченко та інші.

Одне з перших досліджень у цьому напрямі здійснив О. І. Мотлях у дисертації «Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій» (2005) [153], де ним надано криміналістичну характеристику кримінальних правопорушень даної категорії як інформаційну модель, що являє собою систематизований опис типових криміналістично значущих ознак, які мають суттєве значення для виявлення та розслідування протиправних дій осіб у сфері комп'ютерних технологій. Серед основних структурних елементів криміналістичної характеристики автор пропонує розглянути такі дані:

– способи вчинення кримінального правопорушення даної категорії (способи безпосереднього доступу до комп'ютерної інформації або операційної системи; способи видаленого (опосередкованого) доступу; способи виготовлення, розповсюдження на технічних носіях шкідливих програм для ЕОТ);

– слідова картина цих кримінальних правопорушень (слідова картина незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж; слідова картина викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем; слідова картина порушення правил експлуатації автоматизованих електронно-обчислювальних систем);

– особа злочинця, мотиви і мета вчинення кримінального

правопорушення (за статистичними даними вітчизняної та зарубіжної практик, вік осіб, які вчиняють комп'ютерні злочини, сягає від 15 до 45 років. Матеріали експертних досліджень визначають, що на момент вчинення протиправних дій вік 33 % злочинців не перевищував 20 років; 13 % – були старші 40 років; 54 % мали вік від 20 до 40 років);

– деякі обставини вчинення кримінального правопорушення (вони залежать від багатьох факторів, зокрема, на що саме була спрямована протиправна дія) [153, с. 13].

Л. П. Паламарчук у дисертаційній роботі «Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (2005) [169] розкрив системне уявлення про способи вчинення цих кримінальних правопорушень, слідову картину незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що розширили і поглибили знання про методику його розслідування. У своїй роботі науковець зазначав, що незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж може вчинятися шляхом отримання інформації в результаті злочинних шахрайських дій. Разом з тим учений оминув у дослідженні вчинення доступу з використанням шахрайських дій.

Згодом, по мірі накопичення емпіричного матеріалу та розвитку загальної теорії криміналістики, розпочалося поступове вивчення методологічних засад розслідування кримінальних правопорушень, що вчиняються з використанням ЕОТ [86; 113; 189; 199; 205; 224].

Що стосується шахрайств, то основи методик розслідування зазначених кримінальних правопорушень були закладені такими науковцями, як А. В. Крижевський, О. Л. Мусієнко, Т. А. Пазинич, С. С. Чернявський тощо.

Так, Т. А. Пазинич у дисертації «Криміналістична характеристика шахрайств та основні положення їх розслідування» (2007) [169, с. 12].

здійснила класифікацію шахрайств, визначила особливості їх криміналістичної характеристики та сформулювала положення і рекомендації щодо розслідування окремих класифікаційних груп шахрайств. Окремо науковець виділила категорію шахрайств, що вчиняються у сферах використання електронних технологій, та проаналізувала основні елементи їх механізму. Ученою наголошено, що шахрайства названої категорії специфічні з точки зору використовуваних засобів і середовища (обстановки), які обумовлюють особливість носіїв інформації про кримінальне правопорушення і, відповідно, виявлення, фіксацію, дослідження і використання доказів.

Автор констатувала, що особливістю цих кримінальних правопорушень є те, що вони можуть бути вчинені в різноманітних сферах суспільного життя, зокрема у побуті, функціонуванні окремих суспільних інститутів, підприємницькій діяльності тощо. Місце безпосереднього вчинення протиправного діяння (місцезнаходження злочинця, засобів вчинення кримінального правопорушення) не співпадає з місцем знаходження потерпілого і настання наслідків кримінального правопорушення, що пов’язано з використанням ЕОТ. Шахрай заволодіває предметом посягання (грошовими коштами) з використанням різноманітних електронних технічних засобів і відповідного середовища (стільникового зв’язку, пластикових платіжних карток, комп’ютерної Інтернет-мережі).

Серед шахрайств, що вчиняються у сферах використання ЕОТ, визначено та розглянуто найбільш типові способи цього кримінального правопорушення: обманне заволодіння грошима громадян-абонентів мобільних мереж шляхом їх переконання у необхідності перерахування певних сум (повідомлення кодів оплачених карток поповнення рахунку) для участі у різного роду акціях; обманне заволодіння чужими коштами шляхом використання підроблених (крадених) пластикових карток; обманне заволодіння грошовими коштами іноземних громадян за допомогою шлюбних сайтів; обманне заволодіння грошовими коштами банків через

комп’ютерну мережу Інтернет шляхом зламу банківської електронної системи захисту інформації, коли гроші переводяться на підставні рахунки в банки різних країн [169].

О. Л. Мусієнко у дисертаційному дослідженні «Теоретичні засади розслідування шахрайства в сучасних умовах» (2008) [156] та у подальшому у своїй монографії [157] наводить теоретичне узагальнення і вирішення наукового завдання, що проявляється в розробленні цілісної наукової концепції розслідування шахрайства в сучасних умовах, яка будується на новітніх положеннях теорії криміналістики та узагальненні кримінальних проваджень даної категорії кримінальних правопорушень. Шахрайство, на думку О. Л. Мусієнка, являє собою своєрідну «інтелектуальну» злочинну діяльність, вчинення якої передбачає, що шахрай у своїй свідомості розробляє різні схеми проведення шахрайської операції. Вченим досліджено психологічний аспект вчинення шахрайства, проведено ґрунтовний аналіз різних видів шахрайства (як традиційних, так і нетрадиційних). Звернено увагу на появу достатньо нових видів шахрайства, зокрема на інтернет-шахрайство. Вченим запропоновано найбільш доцільні та ефективні першочергові слідчі (розшукові) дії. Встановлено їх особливості при розслідуванні шахрайства та надано характеристику. При розслідуванні шахрайства О. Л. Мусієнко зазначає, що слідчі (розшукові) дії, оперативно-розшукові та організаційно-технічні заходи завжди повинні використовуються у певних комплексах [156].

А. В. Крижевський у дисертації «Криміналістична характеристика шахрайств у сфері мобільного зв’язку» (2012) [117] здійснив комплексний аналіз механізму вчинення шахрайств у сфері мобільного зв’язку, класифікував різноманітні злочинні прояви за предметом злочинного посягання на окремі групи, а також визначив основні елементи криміналістичної характеристики та основні напрями удосконалення діяльності з розкриття та розслідування.

С. В. Самойлов у дисертації «Розслідування шахрайств, учинених із

використанням мережі «Інтернет»» (2014) [207–208] дослідив 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.

Також розслідуванню окремих видів шахрайств присвячено дослідження О. В. Курмана «Методика розслідування шахрайства з фінансовими ресурсами» (2002) [137], С. В. Головкіна «Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування» (2008) [54–55], С. С. Чернявського «Теоретичні та практичні основи методики розслідування фінансового шахрайства» (2010) [248–249], Т. В. Охрімчук «Криміналістична характеристика шахрайства з фінансовими ресурсами та основні напрями розслідування» (2011) [166], А. І. Анапольської «Розслідування шахрайств і пов’язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків» (2011) [14], С. М. Князєва «Розслідування шахрайства, вчиненого способом фінансової піраміди» (2012) [102], Н. Ю. Кириленко «Методика розслідування шахрайства у сфері побутових відносин» (2013) [97].

Окремі напрацювання щодо вдосконалення наявних методик розслідування окремих видів шахрайств, що відповідають сучасним потребам слідчої практики, були відображені у наукових працях Н. М. Ахтирської [18], К. В. Воробйової [53], Т. О. Мудряка [154], А. А. Патика [172] тощо.

Що стосується наукових робіт, присвячених дослідженням проблем здійснення окремих процесуальних дій під час розслідування кримінальних правопорушень, які вчиняються з використанням ЕОТ, то тут необхідно відмітити праці окремих науковців.

Так, В. А. Коршенко у роботі «Теоретичні та методичні основи судової

телекомунікаційної експертизи» (2017) [114] комплексно дослідив концептуальні засади та сформулював рекомендації щодо наукових основ, загальних методичних і організаційних положень судової телекомунікаційної експертизи. На думку науковця, судово-телекомунікаційна експертиза є дослідженням експерта на основі спеціальних знань у галузі електроніки і телекомунікації систем, засобів, мереж та їх складових частин, інформації, що ними передається, приймається, обробляється та містить фактичні дані про обставини кримінального правопорушення, що мають значення для кримінального провадження. Завданням судової телекомунікаційної експертизи є діагностика (встановлення стану об'єкта, механізму, наслідку змін та ін.) та ідентифікація (ототожнення конкретного засобу, програми, користувача мережі тощо). Науково обґрунтоване вчення про сутність судової телекомунікаційної експертизи є підґрунтям для подальших розробок проблем використання спеціальних знань під час розслідування кримінальних правопорушень, що вчиняються з використанням ЕОТ, зокрема і шахрайств [114].

Слушною вважаємо думку О. М. Моїсеєва, що при розслідуванні шахрайств, учинених з використанням ЕОТ, зокрема й кіберзлочинів, дослідження комп'ютерної техніки доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою. Адже докази, що пов'язані з комп'ютерними кримінальними правопорушеннями, які були вилучені з місця події, можуть бути легко змінені як в результаті помилок при їх вилученні, так і в процесі самого дослідження [152].

Саме тому, на думку О. М. Миколенко, і ми з ним погоджуємося, незважаючи на де-юре, відсутність законодавчої вимоги про обов'язкове призначення експертизи в цих провадженнях, де-факто, без призначення і проведення експертизи не можна говорити про ефективне розслідування таких справ [149].

А. С. Білоусов, здійснюючи у 2008 р. криміналістичний аналіз об'єктів

комп’ютерних кримінальних правопорушень в межах вчення про криміналістичну характеристику кримінальних правопорушень, акцентував увагу на необхідності використання спеціальних знань у розслідуванні комп’ютерних кримінальних правопорушень і потребі в проведенні комплексних досліджень комп’ютерних об’єктів, доповнив перелік основних завдань, що ставляться перед спеціалістом в разі його участі у проведенні слідчих дій у справах цієї категорії. У разі вчинення кримінальних правопорушень з використанням інформаційних технологій, їх сліди мають істотні особливості, пов’язані з тим, що вчинення кримінального правопорушення у більшості випадків має за мету вплив на комп’ютерну інформацію. Вчинення таких 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 [33, с. 5].

Водночас сучасні науковці (А. С. Білоусов, О. Л. Мусієнко, С. В. Самойлов, В. В. Тіщенко, С. С. Чернявський та ін.) наголошують на необхідності розробки комплексної методики розслідування шахрайств, учинених з використанням ЕОТ, так як практика розслідування свідчить, що в кримінальному середовищі складаються складні схеми злочинної діяльності. Це положення створює потребу в розробці загальних методико-криміналістичних рекомендацій з розслідування цих кримінальних правопорушень на основі їх узагальнених криміналістичних характеристик [208; 235, с. 64]. Під криміналістичною методикою розкриття і розслідування комп'ютерних кримінальних правопорушень В. О. Голубєв розуміє сукупність наукових положень і рекомендацій, розроблених на їх основі, тобто, науково обґрунтованих і апробованих на практиці порад щодо розкриття й розслідування даних кримінальних правопорушень [58, с. 65].

Низку методичних рекомендацій було присвячено способам встановлення

місцезнаходження ЕОТ, з використанням якої вчинялися кримінальні правопорушення. Серед яких можна відмітити наступні: «Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту (2014) [224], «Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів» (2016) [38], «Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет медійного контенту провайдерами програмних послуг та Інтернет-провайдерами» (2017) [226], «Розслідування кримінальних правопорушень, вчинених у сфері захисту інтелектуальної власності з використанням мережі Інтернет» (2021) [229].

Підсумовуючи викладене у підрозділі, варто зазначити, що сучасний стан боротьби з шахрайствами, учиненими з використанням ЕОТ, визначив для криміналістики низку невирішених завдань. Найбільш суттєві з них – у галузі криміналістичної методики, оскільки саме тут відзначається основне відставання рівня науково-методичних рекомендацій від потреб практики. Йдеться не лише про відсутність методик розслідування «нових» кримінальних правопорушень, а й про застарілість підходів до розслідування тих діянь (зокрема, шахрайства), що, зберігаючи стару кримінально-правову форму, значно змінилися змістовно. Нині у криміналістиці розробка окремих методик ведеться за шаблоном, у якому практичний аспект, нерідко, взагалі відсутній, тоді як їх основою повинні бути саме методи, адаптовані до рівня сприйняття конкретним користувачем.

Наразі є об'єктивна потреба в узагальненні та впорядкуванні наявних методичних рекомендацій щодо розслідування шахрайств, учинених з використанням ЕОТ, з метою формування комплексної криміналістичної методики. Об'єднані в єдиній класифікаційній групі ідеї і теоретичні положення стають цілісною теоретичною концепцією. В основі цієї концепції – характеристика різних видів кримінальних правопорушень, урахування якої дозволяє об'єднати окремі рекомендації в єдину методику. До допоміжних компонентів цієї концепції відносимо положення криміналістичної

класифікації кримінальних правопорушень, криміналістичну характеристику кримінальних правопорушень, теорію криміналістичного прогнозування та ін.

Таким чином, можна зазначити, що вивчення проблем розслідування шахрайств, учинених з використанням ЕОТ, на рівні дисертаційних робіт не проводилось, що і обумовлює його актуальність.

1.2 Предмет злочинного посягання та способи шахрайств, учинених з використанням електронно-обчислювальної техніки

У системі криміналістичної характеристики шахрайства, вчиненого з використанням ЕОТ, важливе значення має предмет злочинного посягання, під яким у ст. 190 КК України [131] розуміється заволодіння 1) чужим майном або 2) придбання права на майно шляхом обману чи зловживання довірою. Отже, виходячи із зазначеного вище, об'єктом шахрайства виступають відносини власності. Предметом шахрайства може бути майно в розумінні речі та право на майно. Важливим є те, що предметом даного кримінального правопорушення можуть бути як рухомі, так і нерухомі речі.

Майно як предмет шахрайства повинно володіти певними фізичними, економічними, юридичними ознаками [80], де:

1) фізичні ознаки – це предмети, речі, які можна вилучити, привласнити, спожити, пошкодити, знищити тощо;

2) економічні ознаки – майно має становити певну матеріальну цінність, мати певну вартість;

3) юридичні ознаки – право на майно належить певному власнику або особі, якій воно на законній підставі ввірено, перебуває у її віданні чи під її охороною, для винного майно є чужим [128, с. 133– 134].

Дослідженню окремих проблем предмета шахрайства присвячували свої праці такі вчені, як П. П. Андрушко, С. Б. Гавриш, В. О. Глушков,

В. Г. Гончаренко, Ю. П. Дзюба, О. О. Дудоров, В. П. Ємельянов, Ю. М. Канібер, М. Й. Коржанський, Л. М. Кривоченко, С. Я. Лихова, П. С. Матишевський, М. І. Мельник, А. А. Музика, В. О. Навроцький, М. І. Панов, О. В. Смаглюк, В. Я. Тацій, В. П. Тихий, Є. В. Фесенко, Ю. Л. Шуляк та інші, які зробили суттєвий внесок у розвиток наукової думки. При цьому значну увагу при розгляді предмета шахрайства автори завжди приділяли ознакам шахрайства, передбаченого ст. 190 КК України, яка міститься у Розділі VI «Злочини проти власності» Особливої частини КК України [131]

Водночас предмет шахрайства, що вчиняється з використанням ЕОТ, як предмет криміналістичної характеристики на даний час практично не відображався у наукових працях та потребує подальшого дослідження [231].

На думку М. І. Панова, В. Ю. Шепітька та В. О. Коновалової, точне встановлення предмета посягання дозволяє відмежувати одне кримінальне правопорушення від іншого, суміжного з ним [171, с. 193].

Аналіз Постанови ПВСУ від 6 листопада 2009 р. № 10 «Про судову практику у справах про злочини проти власності» дозволяє нам стверджувати, що предметом шахрайства є майно, яке має певну вартість і, як уже зазначалося вище, є чужим для винної особи: речі (рухомі й нерухомі), грошові кошти, цінні метали, цінні папери тощо [184].

Стаття 177 Цивільного кодексу України під об’єктами цивільних прав розуміє речі, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні і нематеріальні блага [245].

Своєю чергою, О. В. Кришевич до предмета шахрайства відносить рухоме майно:

а) коштовні речі різного призначення – автомобілі, коштовності, відео- та аудіотехніку та інше, гроші, зокрема у валюті, цінні папери, кольорові метали;

б) гроші, вилучені з обігу, але які підлягають обміну та знаходяться в обігу в банківській чи іншій системі;

в) гроші, давно вилучені з обігу, але які представляють яку-небудь цінність і певну вартість, наприклад, зроблені з дорогоцінних металів, що представляють історичну цінність – рідкі або дуже старовинні й т. ін.

г) безготівкові гроші, що зберігаються на рахунках у банках і кредитних організаціях;

д) цінні папери, зокрема, іменні [135, с. 184–186].

Залежно від обставин, предметом шахрайства можуть також бути:

а) проїзні квитки на транспорт і транспортні абонементи, за винятком іменних квитків і бланків квитків, що вимагають додаткового оформлення;

б) квитки та абонементи на відвідування театральних спектаклів, концертів, кіносеансів, циркових та інших вистав, виставок і т. ін.;

в) квитки різних лотерей (грошово-речових лотерей та ін.);

г) знаки поштової оплати (конверти, марки, листівки тощо);

д) жетони, що заміняють гроші (наприклад, жетони на оплату таксофонів, метро і т. ін.);

е) оплачені магазинні чеки;

є) талони на пально-мастильні матеріали та ін. [135, с. 189].

При цьому О. В. Кришевич із предметів шахрайства, які відносяться до рухомого майна, виключає такі:

а) ядерні матеріали й радіоактивні речовини;

б) вогнепальну зброю, комплектуючі деталі до неї, боєприпаси, вибухові речовини й вибухові пристрої;

в) ядерний, хімічний, біологічний та інші види зброї масового ураження, матеріали та устаткування, які можуть бути використані при створенні зброї масового ураження;

г) наркотичні засоби й психотропні речовини.

Шахрайські дії з цими предметами, передбачені іншими статтями КК України [131; 135, с. 186].

Під нерухомим майном О. В. Кришевич, посилаючись на цивільне законодавство, розуміє:

а) земельні ділянки, ділянки надр, відособлені водні об’єкти та все, що міцно пов’язане із землею, тобто об’єкти, переміщення яких без збитку, нерозмірного їх призначенню, неможливе, у тому числі ліс, багаторічні насадження, будинки, споруди;

б) предмети державної реєстрації, повітряні й морські судна, судна внутрішнього плавання, космічні об’єкти;

в) надра в межах території України, включаючи підземний простір і корисні копалини, що перебувають у надрах, енергетичні та інші ресурси.

Розкрадання подібних об’єктів нерухомості, таким чином, можливе не на рівні розкрадання майна, а тільки на рівні розкрадання прав на нього. Про розкрадання може свідчити лише офіційний переказ права на нерухомість на ім’я винного або осіб, на яких він вкаже [131; 135, с. 186–187].

Своєю чергою, О. В. Тарасова та Л. В. Борисова до предмета посягання шахрайства відносить інформацію, яка може поділятися на:

а) особисту конфіденційну інформацію, якою може бути таємниця листування, телефонних розмов, поштових, телеграфних чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер; таємниця всиновлення; особисте життя особи та його таємниця; інформація, яка є об’єктом авторських і суміжних прав; персональні дані, тобто інформація, яка безпосередньо порушує права та свободи громадян; адвокатська таємниця; лікарська (медична) таємниця; таємниця страхування;

б) конфіденційна інформація юридичних осіб: службова таємниця; комерційна або банківська таємниця; редакційна і журналістська таємниця;

в) державна конфіденційна інформація, тобто інформація, яка належить державі чи його суб’єктам: службова таємниця; дані досудового слідства; відомості про заходи безпеки, що застосовуються по відношенню до посадової особи правоохоронних органів або контролюючого органу;

г) інша категорія інформаційних ресурсів – інформація загального

користування для необмеженого кола осіб тощо [34, с. 42; 231].

Останнім часом збільшилася кількість випадків заволодіння інформацією про власників платіжних банківських карток та їх реквізити. До такої інформації, як правило, належить:

а) ім’я та прізвище держателя картки;

б) назва/код структурного підрозділу банку, що випустив картку;

в) термін дії картки;

г) номер картки.

При цьому необхідно констатувати, що вчинення шахрайства з використанням ЕОТ здійснюється не на нормальне функціонування електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, а на суспільні відносини власності з приводу майна, грошей та інших цінностей, з метою заволодіння якими вчиняється шахрайство. Предметом розглядуваного шахрайства не можуть бути електронно-обчислювальні машини (комп’ютери), системи та комп’ютерні мережі і мережі електрозв’язку. Щодо суб’єктів цих відносин, то подібне шахрайство може бути вчинено будь-якими особами, що використовують електронно-обчислювальні машини (комп’ютери), системи та комп’ютерні мережі та мережі електрозв’язку у власних інтересах, а також особами, які надають відповідні послуги у цій сфері. При цьому, вчиняючи шахрайство, ці суб’єкти здійснюють цілком законні операції з ЕОТ, не порушуючи нормального функціонування електронно-обчислювальних машин [231].

У сучасному світі, пов’язаному з бурхливим розвитком науково-технічного прогресу, шахрайство набуває все більшого поширення, при цьому впливає майже на всі сфери суспільного життя. У зв’язку з недостатнім науковим дослідженням сучасних способів шахрайств, учинених шляхом незаконних операцій з використанням ЕОТ, виникає багато труднощів як у правоохоронних органів, так і судів у процесі розкриття, розслідування та правильної правової кваліфікації цих діянь.

У криміналістичній науці вважається загальноприйнятим той факт, що спосіб учинення кримінального правопорушення є основоположним ті системоутворюючим елементом криміналістичної характеристики, що характеризує будь-який злочин, зокрема і шахрайство, вчинене шляхом незаконних операцій з використанням ЕОТ [71]. При володінні інформацією про спосіб вчинення кримінального правопорушення з'являється можливість висувати обґрунтовані версії про зміст інших елементів криміналістичної характеристики конкретного кримінального правопорушення. Спосіб кримінального правопорушення сприяє встановленню зв'язку злочинця з ознаками інших елементів, він має комплексну структуру, в якій, поряд з правовими елементами характеристики діяння (дії, бездіяльності, провини) злочинця, велике місце належить аналізу процесуальних форм доказування і методики збирання інформації криміналістичними засобами стосовно тієї чи іншої групи кримінальних правопорушень. Встановивши спосіб кримінального правопорушення, слідчий може визначити особу, яка його вчинила. Дуже рідко вдається розкрити кримінальне правопорушення, якщо невідомий спосіб його вчинення, а його встановлення є ключем до виявлення доказів, характерних саме для даного способу. Виявлення способу кримінального правопорушення допомагає розкривати причини та умови, що сприяють його вчиненню [187, с. 41].

Це є саме стосується і способу шахрайств, учинених з використанням ЕОТ, що викликає необхідність звернути на дане питання особливу увагу як в теоретичному, так і практичному плані.

Вченню про спосіб кримінального правопорушення в різний час приділяли увагу в наукових дослідженнях Ю. П. Аленін, В. П. Бахін, Р. С. Бєлкін, В. Ф. Єрмолович, С. М. Зав'ялов, Г. Г. Зуйков, Н. І. Клименко, Б. М. Ковріжних, О. Н. Колесніченко, В. П. Колмаков, В. О. Коновалова, Е. Д. Куранова, Г. М. Мудьюгін, М. І. Панов, М. А. Погорецький, М. В. Салтевський, В. Ю. Шепітько та інші.

Поряд з цим окремі криміналістичні особливості способів шахрайств, учинених шляхом незаконних операцій з використанням ЕОТ, розглядали у своїх наукових працях Р. С. Атаманов, С. М. Князєв, Т. А. Пазинич, В. П. Сабадаш, М. М. Федотов, С. С. Чернявський.

Не дивлячись на те, що проведені ними дослідження є вагомим внеском у вивчення особливостей способу вчинення даного кримінального правопорушення та сприяють його розслідуванню, проблема способу вчинення кримінального правопорушення як одна з ключових у кримінальному праві й криміналістиці залишається як і раніше дискусійною, при цьому в практичній діяльності слідчих НП виникають проблеми в розкритті, розслідуванні та правильній кваліфікації, що потребує більш глибокого й комплексного наукового дослідження способів учинення шахрайств шляхом незаконних операцій з використанням ЕОТ. Це зумовлено, насамперед, розходженням об’єктів дослідження та завдань, на вирішення яких вони спрямовані. Для криміналістики на перший план виступають ознаки способу вчинення кримінального правопорушення, які відображаються у комплексі різноманітних матеріальних та ідеальних слідів, що дозволяє зорієнтуватися у вчиненому діянні й намітити найбільш оптимальні методи його розслідування [45, с. 28].

У криміналістичній теорії представлено різні погляди стосовно визначення способу вчинення кримінального правопорушення. Для початку зазначимо, що спосіб – це певна дія, прийом або система прийомів, яка дає можливість зробити, здійснити що-небудь, досягти чогось; те що служить знаряддям, засобом і таке інше у якій-небудь справі, дії [42, с. 1375].

Як зазначає В. Ю. Шепітько, спосіб кримінального правопорушення являє собою збірне поняття. Його структура охоплює: способи готування до злочинного діяння, способи його вчинення і способи приховання (маскування).

М. В. Салтевський вказує, що спосіб вчинення кримінального правопорушення – це комплекс динамічних актів рухів, що залишають у

навколишньому середовищі зміни – сліди кримінального правопорушення, які є джерелом інформації для розслідування кримінального правопорушення, виявлення і викриття винних [201, с. 424]. При цьому спосіб кримінального правопорушення не завжди має повну структуру, адже існують кримінальні правопорушення, які можуть вчинятися без попередньої підготовки або не мають на меті наступне приховання події чи слідів [170, с. 215].

В. П. Бахін зазначає, що спосіб вчинення кримінального правопорушення – це вираження та відображення образу дії злочинця під час вчинення ним протиправних діянь [23, с. 178–182].

Своєю чергою, Р. С. Бєлкін вважає, що дані про спосіб вчинення та приховування кримінального правопорушення є центральною частиною криміналістичної характеристики, оскільки вони висвітлюють функціональний бік злочинної діяльності. Він зазначає, що такі дані включають в себе не тільки операціональні відомості (яким шляхом підготовляється, вчиняється та приховується злочин), а й дані про те, як дії злочинця відображаються в навколишньому середовищі, тобто які сліди, «відбитки» дій злочинця виникають у результаті злочинного посягання [118, с. 688–689].

На думку А. Н. Колесниченка та В. О. Коновалової, під способом кримінального правопорушення необхідно розуміти образ дій злочинця, що виражається в певній, взаємозалежній системі операцій і прийомів підготовки, вчинення і приховування кримінального правопорушення [106, с. 22].

Окремі способи шахрайств, вчинених з використанням ЕОТ, розкривають у свої працях І. Г. Андрущенко, О. В. Кришевич, Ю. І. Пивовар, О. В. Рівчаченко, О. М. Стрільців. Зокрема, таке кримінальне правопорушення має місце тоді, коли така операція є способом вчинення цього кримінального правопорушення (унаслідок вішингу (телефоне шахрайство з виманюванням реквізитів банківських карток і переказом

коштів на карту злодіїв з рахунків українців), а внаслідок фішингу (виманювання конфіденційних даних – паролів, номерів банківських карток, PIN-кодів), шахрайства з використанням банкоматів: компрометації даних (скімінг і Івс-дроппінг), захоплення готівки (кеш-треппінг) [3].

Способи шахрайств, учинених з використанням ЕОТ, О. В. Кришевич пропонує диференціювати на три основні групи:

1) способи незаконного доступу до банківських рахунків, пов'язані з використанням розрахунків платіжними дорученнями;

2) способи вчинення кримінальних правопорушень, пов'язаних з 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. 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 [136].

Підсумовуючи погляди вчених щодо визначення способу вчинення кримінального правопорушення, зазначимо, що накопичення знань про спосіб вчинення шахрайства з використанням ЕОТ слугує засобом для розкриття його картини та механізму, встановлення винуватих осіб за результати відбиття злочинних дій у слідах-наслідках, які є важливим джерелом відомостей про злочинну поведінку.

Разом з тим необхідно відмітити, що спосіб вчинення кримінального правопорушення у криміналістичному значенні є ширшим, ніж у кримінально-правовому, тому що характеризує не лише суспільно небезпечне діяння, назване у диспозиції, але й усю злочинну діяльність. При цьому, вчинення кримінального правопорушення може характеризуватися не одним, а комплексом способів (названих або не названих у складі

кримінального правопорушення) [260, с. 332]. Шахрайство, як заволодіння чужим майном або придбання права на майно, здійснюється шляхом обману чи зловживання довірою.

Різновидом шахрайського обману судова практика визнає фіктивне представництво, за якого винний, створюючи враження про свою належність до того чи іншого підприємства, має на меті укласти договори й отримати гроші без поставки товару або, навпаки, одержати товар без належної його оплати. До найбільш поширених випадків застосування обману як способу шахрайства належать: учинення різних угод щодо рухомого і нерухомого майна (купівля-продаж, оренда), коли потерпілому передається фальсифікований товар або предмети гіршої якості, або ж предметом угоди виступають фіктивні предмети, які не існують в об'єктивній реальності або не належать винній особі; незаконне отримання пенсій, субсидій, інших видів соціальної допомоги на підставі підроблених документів; обманне отримання попередньої оплати (авансу) за надання товарів чи послуг [93, с. 245].

Як слушно зазначає Т. А. Пазинич, обман під час шахрайства – поведінка особи, яка свідомо спрямована на те, щоб будь-якими засобами сформувати в іншої людини уявлення, яке не відповідає дійсності, й спонукати її до передачі майна або права на нього [167, с. 7].

Сутністю обману, на думку К. Л. Попова, є дезінформування жертви, рефлексивне управління суб'єктом кримінального правопорушення процесом прийняття жертвою певних рішень [175, с. 10].

Обман може мати місце щодо предмета (його ціни, якості, кількості і т. п.), особи (її службового або громадського стану, професії) тощо. Зловживання довірою під час шахрайства є своєрідною формою обману, що полягає в недобросовісному використанні злочинцем певних відносин, які вже склалися між ним і потерпілим. Така форма обману може виникнути тоді, коли між потерпілим і винною особою вже існують відносини, які і породжують певну, можливо тільки 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 [238, с. 385].

При цьому О. М. Мельник зазначає, що при вчиненні шахрайства з використанням ЕОТ, в оману вводиться саме людина, яка є безпосереднім користувачем відповідних технічних засобів і діяльність якої пов'язана з використанням результатів їх обчислень [148, с. 60].

І. О. Руденко під обманом, як спосіб вчинення шахрайства шляхом незаконних операцій з використанням ЕОТ, розуміє інформаційний, інтелектуальний вплив шахрая на свідомість і психіку жертви шахрайства через застосування засобів ЕОТ з метою спонукати потерпілого до добровільної передачі майна або права на нього на користь шахрая. Отже, при вчиненні такого кримінального правопорушення обманний вплив на свідомість і психіку потерпілого чиниться опосередковано [200, с. 109–110].

Важливим недоліком вище вказаних публікацій є те, що вони в більшості випадків забувають про другу сторону шахрайства, а саме зловживання довірою, під яким юридична практика розуміє «недобросовісне використання довіри потерпілого з метою викликати у потерпілого впевненість у вигідності чи обов'язковості передачі їй майна або права на нього» [184]. Як шахрайство, учинене в спосіб зловживання довірою, потрібно розглядати отримання кредиту, попередньої оплати за товари чи виконання робіт (авансу), укладення договору позики, укладення договору прокату тощо без наміру повернути отримані кошти чи інші матеріальні цінності, виконати відповідну роботу, повернути борг чи отримані в користування речі [107].

Дослідження способів учинення шахрайств шляхом незаконних операцій з використанням ЕОТ, на думку С. С. Чернявського, виступає своєрідним «ключем» до описання інших значущих елементів криміналістичної характеристики [248, с. 9]. Проте способи вчинення шахрайств шляхом незаконних операцій з використанням ЕОТ значно відрізняються від способів учинення інших кримінальних правопорушень,

пов’язаних із шахрайством, які необхідно відмежувати, зокрема: завдання майнової шкоди шляхом обману або зловживання довірою (ст. 192 КК України); шахрайства з фінансовими ресурсами (ст. 222 КК України); несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв’язку (ст. 361 КК України); несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України).

Як показує аналіз слідчої та судової практики, для шахрайств, учинених шляхом незаконних операцій з використанням ЕОТ, більш характерна така форма вчинення, як заволодіння грошовими коштами (Додатки Б, В).

Власний практичний досвід, аналіз слідчої практики (Додаток В), а також дослідження наукових праць А. І. Анапольської [14], О. Л. Мусієнка [156], Т. А. Пазинича [167], С. В. Самойлова [207], С. С. Чернявського [250], вивчення інших наукових публікацій та слідчо-судової практики дозволив виокремити декілька типових способів шахрайств, учинених з використанням ЕОТ, які нині розповсюджені на території України. Зупинимось на найбільш поширених в Україні.

Фішинг (англ. Phishing) – один з методів шахрайства з використанням соціальної інженерії, який полягає в тому, що зловмисники, імітуючи діяльність реально існуючих компаній або банків-емітентів, використовуючи неголосові засоби комунікації, під різними приводами виманюють у власників платіжних карток реквізити та іншу конфіденційну інформацію. Різновидами фішингу є: 1) фішингові сайти; 2) фішингові електронні листи; 3) фішингові SMS-повідомлення. Крадіжка персональних даних користувача кредитної картки та даних про саму кредитну картку. Метою злочинців у даному випадку є особисті дані, такі як імена, адреси електронної пошти

користувача кредитної картки, а також дані кредитних карт або інформація про акаунт (рахунку). У подальшому це дозволяє злочинцям, наприклад, здійснювати замовлення товарів в Інтернеті під чужим ім'ям і оплачувати їх, використовуючи чужу кредитну карту або списання коштів з чужого рахунку [159].

Для прикладу. «16 грудня 2014 р. ОСОБА_2, маючи злочинний умисел на заволодіння грошовими коштами держателів платіжних карт, шляхом несанкціонованого їх списання через системи on-line платежів, розуміючи, що для досягнення свого злочинного умислу йому потрібні спільники, на роль яких підшукав ОСОБА_3 та ОСОБА_1, який, своєю чергою, до даної протиправної діяльності залучив ОСОБА_4. В результаті, будучи об'єднаними єдиним умислом, між ними були розподілені злочинні функції наступним чином: собі ОСОБА_2 відвів роль здійснювати телефонні дзвінки потенційним потерпілим та в шахрайський спосіб довідуватись в них реквізити банківських карток, відкритих на їхнє ім'я; ОСОБА_1 доручено підшукати особу, яка б мала доступ до мережі Інтернет і могла здійснити операції по переказу коштів у системі on-line платежів iPay.ua. Своєю чергою, ОСОБА_1, через ОСОБА_5, ІНФОРМАЦІЯ_2 підшукав ОСОБА_6, ІНФОРМАЦІЯ_3, якого не поставив до відома про дійсність своїх злочинних намірів. Переказ грошових коштів, здобутих злочинним шляхом, у готівку відводився ОСОБА_3 та ОСОБА_4 , які згідно з вказівками ОСОБА_2 та ОСОБА_1, повинні будуть здійснити відповідні операції із зазначеними коштами.

Так, діючи відповідно до узгодженої всіма учасниками злочинної змови плану, 16 грудня 2014 р. о 8 год. 50 хв. ОСОБА_2 зателефонував на мобільний телефон НОМЕР_1, що належить потерпілому ОСОБА_7, та представившись працівником служби безпеки ПАТ КБ «ПриватБанк», тим самим повідомив неправдиву інформацію, яку потерпілий сприйняв за дійсну. В подальшому ОСОБА_2, зловживаючи довірою потерпілого ОСОБА_7, отримав відомості, щодо реквізитів банківської картки ПАТ КБ «ПриватБанк» № НОМЕР_2, а саме строку дії карти, CVV код, після цього, вказані реквізити повідомив ОСОБА_8, а той, своєю чергою, став консультувати ОСОБА_6 , який в цей час

знаходився за місцем свого проживання за адресою АДРЕСА_2 та користувався комп'ютерною технікою, підключеною до мережі Інтернет (провайдер ТОВ «Воля-Кабель»). Останній чітко діючи за вказівкою ОСОБА_8, здійснив доступ до web-ресурсу iPay.ua, де заповнив поля для проведення транзакцій реквізитами, вказаними йому ОСОБА_8. В результаті чого, на номер мобільного телефону ОСОБА_7 з банківського номеру НОМЕР_3 надійшли «смс» повідомлення з восьмизначними одноразовими паролями. Будучи введеним в оману, ОСОБА_7 продиктував їх ОСОБА_2, а він, своєю чергою, ОСОБА_8, той, відповідно, ОСОБА_6. Останній, не будучи обізнаним про факт неправомірного зняття коштів, фактично здійснив транзакції про їх списання з карткового рахунку потерпілого ПАТ КБ «ПриватБанк» № НОМЕР_2 на картковий рахунок № НОМЕР_4 ОСОБА_3, ІНФОРМАЦІЯ_4, здійснивши дві операції: о 9 год. 11 хв. на суму 2905 грн та о 9 год. 15 хв. на суму 2905 грн. Також, на картковий рахунок № НОМЕР_5 ОСОБА_4 здійснено дві операції: о 9 год. 26 хв. на суму 2905 грн. та 9 год. 29 хв. на суму 1205 грн, а також одну операцію по поповненню мобільного номера НОМЕР_6 на суму 298 грн 08 коп. В подальшому вказані грошові кошти було знято готівкою ОСОБА_3 в банкоматі за адресою АДРЕСА_3 та ОСОБА_4 в банкоматі за адресою АДРЕСА_4, якими вони розпорядились відповідно до вказівок ОСОБА_2 та ОСОБА_1, а також на власний розсуд. ОСОБА_4, ОСОБА_3, ОСОБА_2, ОСОБА_1 завдали своїми умисними протиправними діями потерпілому ОСОБА_7 матеріальної шкоди на загальну суму 10 218 грн 08 коп.» [48].

Створення інтернет-аукціонів шляхом надання недостовірних даних та пропозиції продажу неіснуючих товарів. Зазвичай злочинці реєструються на вебсайтах інтернет-аукціонів, частіше всього на «Aukro.ua», «Емаркет Україна» (olx.ua). При цьому шахраї використовують анкетні дані близьких або сторонніх осіб. Після чого на сайті, під своїм доменним іменем, розміщують лот, до якого завантажують фото товару з максимальною вартістю та початковою ставкою, де учасники інтернет-аукціону, потенційні жертви, дистанційно ставлять ставки на сайті вказаного товару. По завершенню торгів, шахрай зв'язується із жертвою на сайті інтернет-

аукціону, однак часто спілкування може здійснюватись шляхом листування електронною поштою або мобільним зв'язком. Після домовленості в ціні, шахрай надає жертві реквізити банківського рахунку для оплати товару та послуг пересилання, однак, в кінцевому результаті, після перерахування коштів жертва товару не отримує. Шахрай, з метою приховання процесу злочинних дій та самовикриття, може використовувати банківські картки інших осіб та в подальшому переводить в готівку шляхом зняття коштів із банкомату. Більш досвідченіші злочинці, з метою приховання свого місця знаходження, постійно змінюють IP-адреси, що створює труднощі у встановленні місця знаходження шахрая [227].

Отримання даних про банківську картку та подальше перерахування коштів з банківських карток потерпілого. Для вчинення вказаного виду шахрайства, шляхом незаконних операцій з використанням ЕОТ, злочинці на сайтах інтернет-торгівлі підшукують жертв. Знайшовши інформацію потенційної жертви про продаж товарів, шахраї встановлюють з останньою контакт. Під час розмови з жертвою шахраї неправдиво повідомляють, що будуть здійснювати купівлю товарів, і для перерахунку грошових коштів за покупку дізнаються номер її банківського карткового рахунку. Після чого шахрай телефонує жертві та, представившись працівником банку, повідомляє інформацію про неможливість перерахунку коштів на карту потерпілої. Після чого, в ході телефонної розмови, неправдиво повідомляють, що для зарахування грошових коштів їй необхідно повідомити конфіденційні дані банківської картки (анкетні дані жертви, захисний код картки і дівоче прізвище матері), або підійти до терміналу банкомата та виконати необхідні операції для нібито зарахування коштів на її банківську картку. Під час розмови по телефону з жертвою шахрай диктує відповідні комбінації, які остання виконує, та шляхом обману і незаконних операцій з використанням електронно-обчислювальної техніки отримує грошові кошти.

У подальшому шахрай, використовуючи електронні платіжні системи мережі Інтернет («Портмоне», ГлобалМані, EasyPay, LiqPay, iPay.ua,

Простір), перераховує грошові кошти з карткового рахунку потерпілої на свій банківський рахунок або рахунок третіх осіб, яким навіть не відомо, що з їхніми банківськими картками проводяться злочинні операції. Для того, щоб жертва відразу не дізналась, що відносно неї вчинено шахрайство, злочинці надсилають на мобільний номер останньої SMS-повідомлення про зарахування коштів на банківську картку [237].

Обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій. При використанні благодійних сайтів злочинці надсилають листи від імені благодійних організацій або людей, яким потрібна допомога. При цьому посилання можуть належати реальним благодійним фондам, але реквізити для перерахування коштів належать шахраям.

Крім цього, злочинці шляхом незаконних операцій з використанням ЕОТ, створюють сайти благодійних організацій, на яких публікують оголошення з проханням про матеріальну допомогу на лікування хворим дітям. Також шахраї на вказаних сайтах можуть розміщувати вигадану інформацію стосовно хвороби, при цьому розміщують чужі фотографії людей, які потребують фінансової допомоги на лікування, або копіюють оголошення з сайтів благодійної допомоги, які належать реальним людям, змінюючи реквізити для перерахування грошей [168, с. 78].

Заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину. Під час створення сайту інтернет-магазину шахрай може діяти як самостійно, так і у складі злочинної групи. Це більш складний спосіб, ніж продаж товарів на інтернет-аукціоні, і складається з декількох етапів. Спочатку шахраї створюють у мережі Інтернет сайти у вигляді інтернет-магазинів – аналогів інтернет-сайтів, що діяли на території України чи інших держав, та які б функціонували на території України. На вказаних сайтах розміщують завідомо неправдиву інформацію у вигляді оголошень щодо продажу товарів, яких в наявності ніколи не було. Наступним етапом є створення та отримання контролю над фіктивними підприємствами,

відкриття банківських рахунків, на які замовники/клієнти фіктивних інтернет-магазинів в подальшому здійснюють передоплату у вигляді грошового переказу за придбання замовленого товару за реквізитами належних їм пластикових карток, відкритих у банках України. При цьому назви фіктивних підприємств повинні бути подібними до назв фіктивних інтернет-магазинів, щоб викликати довіру у користувачів.

Після чого здійснюється оформлення договорів з операторами телефонного зв'язку про надання послуг зв'язку та інтернет-зв'язку, так званої «SIP-телефонії», телефонні номери яких слугують для зворотного зв'язку із замовниками інтернет-магазинів. При цьому у вхідних дзвінках на телефони замовників фіктивних інтернет-магазинів відображаються міські номери телефонів, що викликає довіру в користувачів.

Для прикладу. *«У невстановлений слідством день і час, у період з червня по серпень 2016 р., ОСОБА_1, маючи навички роботи з комп'ютерною технікою та інтернет-ресурсами, з використанням електронно-обчислювальної техніки персонального комп'ютера, знаходячись в м. Житомирі, використовуючи свій обліковий запис, зареєстрований на сайті інтернет-оголошень «http://kloomba.com», «https://ukrrover.jimdo.com», «http://klubok.com», та сайті Інтернет оголошень «http://OLX.ua», з метою подальшого незаконного заволодіння коштами потенційних клієнтів шляхом обману, розмістив на вказаних сайтах оголошення на продаж різноманітних товарів, які насправді не мав наміру продавати, в результаті чого вчинив низку умисних, корисливих кримінальних правопорушень за наступних обставин.*

27 червня 2016 р. ОСОБА_2 (м. Буча, Київської області) у всесвітній мережі загального доступу «Інтернет» переглядала сайт оголошень «http://OLX.ua» та побачила оголошення про продаж дитячого біговела вартістю 700 грн 00 коп., яке розмістив користувач вказаного вище сайту, при цьому зазначив свій контактний номер мобільного телефону НОМЕР_1. Після цього, ОСОБА_2, будучи введеною в оману користувачем номера

мобільного телефону НОМЕР_1 , який належить ОСОБА_1, домовилася про купівлю вказаного товару, при цьому ОСОБА_1, маючи умисел, спрямований на заволодіння чужим майном шляхом обману, повідомив ОСОБА_2, що умовою передачі товару є лише 100-відсоткова оплата його вартості.

На виконання вказаних домовленостей ОСОБА_2 27 червня 2016 р., будучи неправдиво запевненою в добросовісності намірів ОСОБА_1, здійснила перерахування готівкових коштів в сумі 700 грн 00 коп. на банківський картковий рахунок № НОМЕР_2, відкритий у ПАТ КБ «УкрСиббанк» на ім'я ОСОБА_1. При цьому, ОСОБА_1 завірив ОСОБА_2, що після перерахування грошових коштів за замовлений товар одразу надішле на ім'я останньої оплачений товар.

Після цього, ОСОБА_1, отримавши грошові кошти в сумі 700 грн 00 коп., порушуючи попередню домовленість, вказаний товар не надіслав, отриманими грошовими коштами розпорядився на власний розсуд.

Таким чином, ОСОБА_1 незаконно, шляхом обману (шахрайство) та незаконних операцій з використанням електронно-обчислювальної техніки, заволодів грошовими коштами ОСОБА_2 в сумі 700 грн 00 коп., чим спричинив останній матеріальної шкоди на вказану суму» [49].

В окремих випадках вчиняються дії зі створення, організації та забезпечення діяльності структурної частини злочинної групи, а саме «кол-центру», оператори якого спілкуються з клієнтами, імітуючи діяльність кол-центрів справжніх інтернет-магазинів, приймають замовлення та надають реквізити для перерахування грошових коштів. Крім цього, шахраї розробляють спеціальну вебсторінку з базою даних для роботи організаторів та операторів «кол-центру», за допомогою якої злочинці приймають та ведуть облік замовлень. Після вчинення шахрайських дій, так звані оператори «кол-центру» заносять телефонні номери ошуканих клієнтів до «чорного списку», щоб вони не заважали роботі «кол-центру» та якнайдовше не здогадувались, що відносно них було скоєно шахрайство.

На завершальному етапі підготовки до вчинення кримінального

правопорушення та під час безпосередньої протиправної діяльності здійснюється підбір чи добір учасників злочинної групи для вчинення шахрайств, шляхом незаконних операцій з використанням ЕОТ [50; 159].

Створення та діяльність фіктивних фінансових бірж. Діяльність таких бірж забезпечується діяльністю злочинної групи, яка складається та маскується за офіційно зареєстрованими підприємствами. Зловмисники використовують методи агітаційного характеру для залучення громадян до інвестування коштів у торгівлю на фінансових ринках. Шахраї пропонують потенційним клієнтам купувати цінні папери для отримання прибутку. Використовуючи бренди «hqbroker» та «trade12», злочинці задіюють різні вебресурси для імітації добросовісної ділової репутації. Після чого так звані «брокери» створюють у потерпілого помилкову уяву про процес здійснення торгів на світових біржах. Для цього вони використовують вже встановлене на комп'ютер потерпілого спеціальне програмне забезпечення для проведення торгів, яке фактично надає можливість здійснювати віддалений контроль за його комп'ютером. Такі компанії створюють уяву у потерпілих про співпрацю з іноземними компаніями, що торгують цінними паперами, які є учасниками фондового ринку та мають відповідні дозволи та ліцензії на здійснення зазначеної діяльності у світі. Такими діями злочинці спонукають потерпілого вносити свої кошти на рахунок шахрайського торгівельно-сервісного підприємства, переслідуючи при цьому мету – заволодіння його коштами під приводом укладання угод з купівлі-продажу цінних паперів [161].

Крім цього, аналогічним способом учасники групи організовують діяльність офісів для «операторів», «технічних працівників» і «брокерів». Такі офіси можуть розміщувати у різних містах. Свою діяльність шахраї «прикривають» офшорною компанією. Для вчинення протиправної діяльності злочинці використовують спеціально створений для цього онлайн ресурс (інтернет-майданчик), де нібито відбувалися успішні онлайн торги валютними парами (бінарні опціони). За схемою, потенціальному клієнту

пропонують взяти участь у торгах шляхом відкриття спеціального демо-рахунку, де організаторами створюється імітація успішних торгів. Після чого, особу шляхом обману скеровують на відкриття реального рахунку. При цьому, з потерпілими працюють «оператори» офісу, які націлюють їх на внесення якомога більших внесків. Аргументують це більшою вірогідністю виграшу. Для досягнення цієї мети зловмисники використовують заздалегідь прописану схему психологічного впливу на жертву. Вклавши гроші, потерпілі не мають можливості їх «зняти». В даному випадку вони можуть лише поповнювати рахунки. Система працює таким чином, що всі торги призводять до повної втрати грошей користувачів [98; 159; 207, с. 7].

Також у 2020 р. набули популярності шахрайські схеми, замасковані під сервіси доставки платформ оголошень. У такому випадку злочинці розміщували оголошення про продаж товарів і для обговорення деталей пропонували перейти у месенджери. Туди покупцям надсилали фальшиві накладні для сплати або посилання на фейковий ресурс, де потрібно оформити доставку. Однак врешті оплата надходила не на платформу оголошень, а на картку шахрая [214].

Аналіз визначених вище та інших способів шахрайства, учинених з використанням ЕОТ, дозволяє поділити їх за наступними критеріями:

1. Залежно від періодичності вчинення кримінального правопорушення:

1) одноразові (шахрайство вчиняється з метою обману однієї визначеної особи з метою заволодіння певним товаром, що належить їй, або сумою грошей за продаж неіснуючого товару). Наприклад, заволодіння коштами шляхом імітування продажу неіснуючого товару шляхом розміщення відповідних повідомлень на сайті OLX.ua;

2) тривалі (шахрайство вчиняється з метою обману невизначеного кола осіб) [126]. Наприклад, шляхом створення сайту з продажу послуг (туристичних) чи товару (медичних масок) невизначеної кількості осіб.

2. Залежно від сфери застосування:

1) банківська (виманювання або інше незаконне отримання конфіденційних даних клієнта банку та подальше перерахування коштів з банківських рахунків й отримання додаткових кредитів);

2) побутова (отримання речей, що дорого коштують, за документами своїх родичів, за викраденими чи знайденими документами);

3) страхування (надання неіснуючих страхових полісів);

4) туристична галузь (надання неіснуючих туристичних послуг);

3. Залежно від кількості задіяних до вчинення шахрайства осіб:

1) вчинено за участю однієї особи;

2) вчинено групою осіб;

3) вчинено організованою групою осіб;

4. Залежно від предмета посягання:

1) грошові кошти;

2) матеріальні цінності:

– побутові предмети;

– рухоме майно, зокрема транспортні засоби;

4) інформація про особистість, акаунт або банківську картку;

5) право на майно, зокрема на нерухоме.

5. Від виду ЕОТ, яка використовувалась:

1) комп'ютери та ноутбуки;

2) телефони;

3) планшети;

4) інші види.

6. Залежно від інформаційної підтримки:

1). цілеспрямоване створення окремого інтернет-сайту;

2) розміщення інформації на вже існуючих інтернет-сайтах;

3) шляхом несанкціонованого доступу до ЕОМ потерпілого;

7. Залежно від характеру «стосунків», що виникають між потерпілим і злочинцем:

1) установчі дані злочинця невідомі;

2) попередні дані про особу-злочинця відомі;

3) відомі попередні дані лише про одну особу, яка діяла у складі групи осіб.

8. Залежно від місця створення та місця реєстрації IP-адреси ЕОТ:

1) місце знаходження встановлено (Україна);

2) місце знаходження – за кордоном (країна та установчі дані провайдера відомі);

3) місце знаходження – тимчасово окуповані території Донецької та Луганської областей або окупованій та у подальшому анексованій Автономній Республіці Крим;

4) місце знаходження країни не встановлено.

9. Залежно від способів введення в оману або зловживання довірою:

1) маніпулювання якістю інформації, тобто фальшування деяких фактів або навмисне укривання істини;

2) маніпулювання кількістю інформації, тобто укриття частини правди або паралельне подання неіснуючих та існуючих фактів як істини;

3) повідомлення двозначної або неконкретизованої інформації;

4) умовчування – повне приховування правди;

5) спотворення – навмисне повідомлення помилкової інформації [139, с. 273–274].

10. За характером подання відомостей:

1) активний (повідомлення потерпілому неправдивих відомостей про певні факти, обставини, події) характер;

2) пасивний (умисне замовчування юридично значимої інформації) характер [93, с. 245].

11. За новизною способу вчинення шахрайства:

1) спосіб обману (зловживання довірою) невідомий у правоохоронній практиці;

2) спосіб обману (зловживання довірою) зустрічався раніше в правоохоронній практиці.

12. За ступенем доведеності кримінального правопорушення:

1) шахрайство частково реалізоване;

2) шахрайство реалізоване;

3) шахрайство припинене.

13. Залежно від способу підготовки до вчинення шахрайства:

1) вчиненню шахрайства сприяв несанкціонований доступ до ЕОТ;

2) вчинення шахрайства здійснювалось з використанням шкідливих програмних чи технічних засобів;

3) вчиненню шахрайства сприяло розповсюдження рекламної чи іншої продукції про предмет посягання (надання послуг).

Підводячи висновки до підрозділу зазначимо, що проведений аналіз судової та слідчої практики дозволив встановити наступні види майна, які були предметом шахрайства з використанням ЕОТ: майно (рухоме, нерухоме); право на майно. Особливістю предмета шахрайства, учиненого з використанням ЕОТ, є заволодіння інформацією про власників платіжних банківських карток та їх реквізити.

Способи шахрайств, учинених з використанням ЕОТ, – це сукупність дій злочинця, що полягає у певному порядку, послідовності та конкретному методі діяльності особи шахрая, спрямованих на підготовку, вчинення та приховування конкретного кримінального правопорушення.

Не існує вичерпного переліку способів вчинення даного кримінального правопорушення, але найбільшого поширення останнім часом набули наступні: обманне заволодіння грошима громадян; створення інтернет-аукціонів шляхом наданням недостовірних даних і пропозиції продажу неіснуючих товарів; створення і забезпечення діяльності інтернет-магазину; перерахування коштів з банківських карток шляхом обманного отримання конфіденційних даних; обманне заволодіння грошовими коштами іноземних громадян; обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій, створення та діяльність фіктивних фінансових бірж. Вказаний перелік способів не є вичерпним, що

зумовлює потребу в подальшому науковому дослідженні.

Своєю чергою, дослідження способів учинення шахрайств з використанням ЕОТ доцільно використовувати в практичній діяльності правоохоронних органів, оскільки воно сприятиме швидкому, повному та всебічному розкриттю і розслідуванню даної категорії кримінальних правопорушень. Таким чином, знання основного елемента криміналістичної характеристики – типових способів шахрайств, вчинених з використанням ЕОТ, – має певне наукове та практичне значення. Знання способу шахрайства дозволяє виявити: безпосередніх виконавців шахрайських дій; обстановку, що сприяла вчиненню кримінального правопорушення; типові сліди протиправної діяльності з використанням ЕОТ.

1.3 Слідова картина та обстановка шахрайств, учинених з використанням електронно-обчислювальної техніки

«Слідова картина» є обов’язковим елементом криміналістичної характеристики кримінальних правопорушень, оскільки її зміст виступає практичним інструментом і своєрідним орієнтиром у виборі напрямів їх розслідування. Термін «слідова картина» – поняття дещо умовне, близьке до поняття «слідова обстановка» або «інформаційне середовище», що включає як матеріальні, так і ідеальні відображення. Таким чином, «слідова картина» (слідова обстановка в широкому її розумінні) як елемент криміналістичної характеристики являє собою абстрактну модель слідів кримінального правопорушення, що відображаються в матеріальному середовищі внаслідок його вчинення [203, с. 150–151].

Зазвичай більшість науковців під типовою «слідовою картиною» кримінального правопорушення в її широкій інтерпретації розуміють сукупність джерел матеріальних та ідеальних відображень у навколишній

матеріальній обстановці вчиненого кримінального правопорушення [137, с. 253].

В. Я. Тацій, М. І. Панов, В. Ю. Шепітько, В. О. Коновалова та інші вчені поділяють «слідову картину» більш ширше:

а) зміни в речовій обстановці;

б) сліди-відображення (сліди рук, ніг, транспорту, інструментів тощо);

в) предмети-речові докази;

г) ідеальні сліди (сліди пам’яті людини);

д) запахові сліди і сліди мікрочастинки [171, с. 194].

Разом з тим характерною ознакою вчинення шахрайств з використання ЕОТ є залишення на місці події одночасно зі звичайними матеріальними слідами іншого виду слідів – віртуальних, що знаходяться в пам’яті електронних пристроїв. Щодо останнього виду слідів, окремі автори ще визначають їх як «електронні цифрові сліди», під якими розуміють матеріальні невидимі сліди, які можуть бути виявлені, зафіксовані й вивчені за допомогою цифрових електронних пристроїв і містять будь-яку криміналістично значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях [6]. Такі сліди утворюються внаслідок вчинення будь-яких дій в інформаційному просторі комп’ютерних та інших цифрових пристроїв, їх систем і мереж [158, с. 305].

Залежно від обставин і способів шахрайства, учиненого з використанням ЕОТ, про вчинення вказаного кримінального правопорушення можуть свідчити наступні слідові картини на місці події, яких може бути декілька:

– місце події потерпілого від вчинення шахрайства;

– місце події, з якого вчинялося шахрайство з використанням ЕОТ.

Слідові картини на місці події, яким, як правило, є місце проживання чи роботи потерпілого від вчинення шахрайства, характеризуються наступними слідами, а саме наявність ЕОТ (комп’ютери, їх системні блоки, ноутбуки), якими користувався потерпілий під час вчинення шахрайства

щодо нього, в якому містяться цифрові сліди, які залишилися внаслідок вчинення такого кримінального правопорушення. Такі цифрові сліди можуть утворюватися:

– на фізичних носіях комп'ютерної інформації (жорсткі диски, компакт-диски, флешкарти, накопичувачі інформації та ін.);

– в оперативному запам'ятовуючому пристрої ЕОТ;

– в оперативному запам'ятовуючому пристрої периферійних пристроїв;

– в електронній поштовій скриньці;

– на інтернет-сайті;

– як профіль у соціальних мережах;

– внаслідок проведення банківських платежів між потерпілим і злочинцем.

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

– ЕОТ (комп'ютери, їх системні блоки, ноутбуки);

– периферійні пристрої (монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, джойстики та інше), комунікаційні прилади комп'ютерів і обчислювальних мереж;

– носії інформації (жорсткі диски, флопі-диски, оптичні диски, флеш-пам'ять, зовнішні HDD);

– 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;

– предмети, отримані в результаті вчинення кримінального правопорушення (речі, гроші, інше майно);

– 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).

Також цифрові сліди можуть утворюватися за результатами спілкування жертви зі злочинцем у вигляді бази даних абонентів операторів зв'язку. Зокрема, важливу криміналістично значущу інформацію можна отримати при вивченні даних електронного листування та сервісів обміну SMS (Short Messaging Service – служба коротких повідомлень). В атрибутах файлів електронних листів міститься дата й час відправлення, електронна адреса відправника, найменування та адреса інтернет-провайдера й інша інформація. Найменування й адресу інтернет-провайдера, за допомогою якого злочинець, підключений до мережі Інтернет, може вільно отримати через спеціальну службу Whois (у мережі Інтернет), зазначивши IP-адресу «атакуючого» комп'ютера. Телефонні дзвінки з мобільного телефону та тексти SMS-повідомлень автоматично фіксуються й накопичуються на сервері оператора мобільного зв'язку та можуть бути отримані слідчим [8, с. 92].

Що стосується цифрових слідів – це сліди у свідомості людини, що являють собою специфічну форму вищого рівня психічного, цілеспрямованого, активного, вибіркового відображення, здійснюваного в чуттєво-раціональній формі, в результаті якого формується відносно адекватний, суб'єктивно-об'єктивний «відбиток» – уявний образ у пам'яті людини, заснований на раніше сприйнятій інформації та є формою збереження відповідної інформації [84, с. 7].

Питанням дослідження проблем боротьби зі злочинами, які вчиняються з використанням цифрових пристроїв, учені-криміналісти приділяють значну увагу. Науковці зазначають, що традиційний розподіл слідів у криміналістиці на сліди в широкому сенсі (результат будь-якої матеріальної зміни первинної обстановки внаслідок учинення кримінального правопорушення) та у

вузькому (відображення під час учинення кримінального правопорушення на одному з об’єктів взаємодії слідів зовнішньої будови іншого об’єкта) практично не охоплює злочини, що вчиняються з використанням цифрових засобів. В окремих працях зазначено, що на сучасному етапі розвитку криміналістики як сліди розглядаються й електронні (цифрові) [6; 123].

Учені дискутують не лише щодо сутності цифрових слідів кримінальних правопорушень, а й стосовно їх найменування (комп’ютерні сліди, віртуальні сліди, електронно-цифрові, інформаційні, комп’ютерно-технічні, електронні, цифрові сліди тощо) [43].

За результатами вчинення шахрайств з використанням ЕОТ залишаються як матеріальні, так і цифрові сліди. Цифрові сліди цих кримінальних правопорушень отримуються під час проведення слідчих (розшукових) та інших процесуальних дій у більшості випадків з пам’яті ЕОТ, а також свідків чи осіб, які вчинили це кримінальне правопорушення чи причетні до його вчинення.

Цифрові сліди шахрайств, учинених з використанням ЕОТ, можуть утворюватися:

– на фізичних носіях комп’ютерної інформації (жорсткі диски, компакт-диски, флешкарти, накопичувачі інформації та ін.), якими користувався злочинець;

– в оперативному запам’ятовуючому пристрої ЕОТ злочинця;

– в оперативному запам’ятовуючому пристрої периферійних пристроїв злочинця;

– в електронній поштовій скриньці злочинця (тут можуть міститися сліди переписки злочинця з потерпілим і, навпаки, а також переписка злочинця з іншими злочинцями);

– на інтернет-сайті, який використовувався злочинцем з метою вчинення шахрайства;

– як профіль у соціальних мережах злочинця («ВКонтакте», «Instagram», «Facebook», «Одноклассники», «Twitter» та ін.);

– внаслідок проведення банківських платежів між потерпілим і злочинцем (рахунок в електронних платіжних системах («Qiwi-гаманець», Perfect Money та ін.);

– під час зняття злочинцем у банкоматах коштів, отриманих злочинним шляхом.

Цифровий слід має певну систему ознак у вигляді окремих інформаційних елементів, які можуть бути записані як на одному, так і на декількох носіях цифрової інформації. Носії таких слідів можуть бути одночасно підключені до декількох цифрових пристроїв, об'єднаних, наприклад, у телекомунікаційну мережу [8, с. 91].

С. В. Чучко зазначає, що проведений ним аналіз матеріалів кримінальних проваджень показав, що у 62 % випадків шахрай і потерпілий зв'язувалися по телефону з метою обговорювання умов угоди купівлі-продажу товарів. Унаслідок чого в пам'яті мобільного телефону, в пам'яті SIM-карти, в пам'яті флеш-карти залишаються цифрові сліди. Це можуть бути: сліди з'єднання, SMS-повідомлення, електронно-цифрові сліди у вигляді фотографій товару тощо [253, с. 27].

Отже, хід тривалого спілкування між шахраєм і потерпілим не є прихованим фактом, а може бути відображений у пам'яті електронних пристроїв, за допомогою яких передається інформація. Так, сліди у вигляді віртуальної переписки з питань купівлі-продажу товарів можуть міститися в електронній скриньці, куди надходить інформація від шахрая. Це можуть бути файли і папки зберігання вхідних та вихідних повідомлень електронної пошти, конфігурації поштової програми тощо [253, с. 27].

Час роботи користувача в мережі Інтернет на певній ЕОТ можна встановити за спеціальним log-файлом (журналом), додаткові відомості про вид, порядок і час підключень користувача до мережі і збіг цих даних з log-файлом провайдера може слугувати вагомим доказом використання саме цієї ЕОТ для вчинення шахрайства [6, с. 172].

В. О. Голубєв стверджує, що встановлення часу вчинення кримінальних правопорушень з використанням ЕОТ не складає великих проблем [57, с. 101], оскільки операційна система електронного пристрою детально стежить практично за кожною важливою операцією, інформація про якй відображається в статистичних файлах. 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.

На сайтах соціальних мереж (наприклад, Facebook, Twitter, LinkedIn, Instagram та ін.) можна виявити електронні сліди у вигляді повідомлень і коментарів осіб, що перевіряються, їх персональних даних (наприклад, електронну адресу), фотознімків і відеозаписів, історію пошукових запитів та ін. Ці сліди містять інформацію про час відвідування сайту і деякі персональні дані користувача (наприклад, його електронну адресу), за якими можна здійснити пошук його номера телефону, дати народження, місця роботи та проживання, визначити коло спілкування та інтереси [6, с. 172].

Так само на сторінці вебсайту також можуть міститися віртуальні сліди (фотографії, відгуки та коментарі стосовно певних лотів, результати переписки між користувачами і продавцями тощо). Сліди можуть міститися й в історії голосових повідомлень і відеодзвінках (відеододатки Skype, Google Hangouts, Zoom тощо). Втім, найцінніша інформація криється у доменній адресі (IP-адреси), що дозволяє встановити місцезнаходження точки доступу до комп'ютера, з якого здійснювалося спілкування [253, с. 27].

Оскільки здебільшого шахраї і потерпілі обирають спосіб електронних розрахунків через електронні платіжні засоби та системи, електронні гаманці, інші види безготівкових розрахунків, у телефоні, в комп'ютері може міститися програмне забезпечення, звідки можна отримати слідову інформацію про проведені банківські операції. За таких обставин банківська

карта, рахунок власника картки або рахунок телефонного номера виступають об’єктом слідоутворення [253, с. 27].

Також носіями віртуальних слідів шахрайства, учиненого з використанням ЕОТ, є очевидці кримінального правопорушення (наприклад, особи, які були присутні під час створення сайту, аканту злочинця, використання ЕОТ з протиправною метою чи інших незаконних дій з ним), при цьому, вони могли не знати подальшу мету цих дій. Таким чином, про вчинення шахрайства можуть свідчити ідеальні сліди, тобто ті сліди, що залишилися в пам’яті людей, і ми можемо отримати їх шляхом проведення допиту особи (свідків, потерпілих, затриманих) [140, с. 70].

Особливістю утворення ідеальних слідів є відсутність прямого контакту між взаємодіючими об’єктами. Оскільки ідеальне відображення здійснюється у формі свідомості, то об’єктом, що відображає, є тільки людина як єдиний його носій. При утворенні матеріальних слідів об’єктом, що відображає, може також бути людина, але тільки як тілесна істота [84].

При допиті, свідок описує не саму подію, а образ дійсності, який зберігся в його пам’яті, що може не збігатися в усіх деталях з реальною подією. Звідси стає зрозумілим, чому свідки, що спостерігали ту саму подію, описують її по-різному [177, с. 39], тобто різним є суб’єктивне відображення. Уявна (образна) форма – суб’єктивна форма психічного відображення [25, с. 75]. Іншими словами, суб’єктивна сутність уявного образу визначається індивідуальністю сприйняття, запам’ятовування й відтворення ідеального відображення.

Ідеальні сліди потребують вжиття відповідних заходів щодо їх перевірки. Так, оцінка слідів пам’яті про спосіб шахрайства, учиненого з використанням ЕОТ, проводиться комплексно з урахуванням слідів інших видів взаємодії, що знаходяться відносно досліджуваного моменту часу в синхронічному або поліхронічному зв’язку.

О. В. Ткач виокремлює певні групи осіб, в пам’яті яких залишаються ідеальні сліди шахрайств, учинених з використанням ЕОТ, тобто таких, що

залишаються в пам’яті підозрюваних, потерпілих і свідків, то їх можна поділити на групи залежно від осіб, які є їх носіями:

1) сліди, що зберігаються у пам’яті осіб, які безпосередньо сприймали обставини вчинення кримінального правопорушення (потерпілий та його родичі, інші особи, які входять до вузького кола спілкування з потерпілим і знаходяться в довірливих чи дружніх стосунках із злочинцем);

2) сліди, що зберігаються у пам’яті осіб, яким відомі обставини, що передували вчиненню шахрайства;

3) сліди, що зберігаються у пам’яті осіб, які безпосередньо бачили весь процес шахрайства чи його складові, учинені з використанням ЕОТ;

4) сліди, що зберігаються у пам’яті осіб, яким відомий підозрюваний у зв’язку із вчиненням ним шахрайства;

5) сліди, що зберігаються у пам’яті осіб, з якими підозрюваний підтримує дружні чи сімейні стосунки (родичі, сусіди, приятелі), і які мають на меті приховати факт причетності підозрюваного до вчинення кримінального правопорушення [236, с. 196].

За наявності ідеальних слідів кримінального правопорушення вони закріплюються у процесуальних документах (протоколах допиту свідків, підозрюваного, потерпілого), на підставі яких вживаються подальші процесуальні дії, спрямовані на ефективне розслідування шахрайства, учиненого з використанням ЕОТ.

Таким чином, ідеальні сліди цих кримінальних правопорушень отримуються під час проведення слідчих (розшукових) та інших процесуальних дій з пам’яті свідків чи осіб, які вчинили це шахрайство чи причетні до нього.

Необхідність внесення обстановки вчинення кримінального правопорушення до елементів криміналістичної характеристики зумовлена тим, що вона є, по суті, відправною точкою розслідування й у багатьох випадках визначає успіх цієї діяльності. Саме тому, проблемі дослідження обстановки вчинення кримінального правопорушення в загальній теорії

криміналістичної методики, а також у методиках розслідування окремих видів кримінальних правопорушень присвячено велику кількість праць видатних фахівців у галузі криміналістики, так і молодих учених.

Разом з тим перед визначенням поняття «обстановка вчинення кримінального правопорушення» необхідно стосовно вказаного визначення звернутися до довідникових джерел на предмет з'ясування поняття «обстановка». Так, зокрема, Великий тлумачний словник сучасної української мови трактує поняття «обстановка» таким чином: «…1. Сукупність умов, за яких що-небудь відбувається…// Становище на місці воєнних дій, зумовлене їх перебігом, співвідношенням бойових сил, їх розташуванням, характером місцевості і т. ін.» [41, с. 820].

У тлумачному словнику української мови «обстановка» визначається як сукупність умов, у яких що-небудь відбувається; умови життя кого-небудь; становище на місці воєнних дій, зумовлене їх протіканням, співвідношенням бойових сил, їх розташуванням, характером місцевості тощо; меблі, оздоби та предмети побуту, якими обставлено й прикрашено приміщення, житло [216].

О. Ш. Якупов зазначає, що обстановка – це ті конкретні й специфічні об'єктивні умови, в яких відбувається суспільно небезпечне посягання [266, с. 96]. Ф. Г. Бурчак і Є. Ф. Фесенко пояснюють її як сукупність передбачених законом обставин, які є зовнішнім оточенням злочинного діяння та характеризуються присутністю людей або певних подій [36, с. 131].

За твердженням І. П. Козаченка, І. О. Харь, В. К. Матвійчука під обстановкою вчинення кримінального правопорушення потрібно розуміти збіг подій і обставин, за яких вчиняється злочин. Вона може бути або необхідною ознакою конкретного складу кримінального правопорушення, або обтяжуючою чи кваліфікуючою [129, с. 66]. П. Л. Фріс зазначає, що обстановка вчинення кримінального правопорушення – це відповідні об'єктивні умови, в яких вчиняється кримінальне правопорушення [241, с. 66]. О. М. Омельчук під обстановкою вчинення кримінального

правопорушення розуміє конкретні об’єктивно-предметні умови, за яких вчиняється кримінальне правопорушення [51, с. 21].

Визначаючи структурні елементи обстановки вчинення кримінальних правопорушень, зауважимо, що їх кількісний та якісний склад буде залежати від видів кримінальних правопорушень. Так, В. Д. Берназ, досліджуючи обстановку вчинення крадіжок, до її структури відносить такі елементи:

а) матеріальне середовище, тобто час, місце, об’єкт, макро- і мікропогодні умови;

б) організаційно-управлінське середовище, тобто виробничо-функціональні об’єкти, правоохоронні елементи;

в) соціально-психологічне середовище: мікроклімат у колективі за місцем роботи, ціннісну орієнтацію, психологічну обстановку за місцем проживання [27, с. 45].

Погоджуючись з Л. Брич, зазначимо, що також потрібно визначитися зі змістом поняття «місце вчинення шахрайства як ознака складу кримінального правопорушення». Для цього потрібно з’ясувати такі питання:

1) чи охоплюється поняттям «місце вчинення кримінального правопорушення» лише місце вчинення шахрайства – розташування ЕОТ за місцем проживання (роботи) злочинця чи за місцем проживання потерпілої особи;

2) чи поширюється поняття місце вчинення шахрайства на місцезнаходження інших ознак складу кримінального правопорушення;

3) як відрізнити випадки, коли певні просторові характеристики є місцем вчинення суспільно небезпечного діяння й, відповідно, самостійною ознакою шахрайства – місцем його вчинення, від випадків, коли ті чи інші просторові характеристики стосуються інших ознак складу шахрайства [35, с. 269].

Таким чином, місце вчинення шахрайства має особливе значення, так як воно є джерелом певних слідів, що відображають механізм злочинної дії, взаємини злочинця та жертви. Водночас при розслідуванні шахрайства місце

вчинення кримінального правопорушення та місце події не завжди становлять єдиний комплекс. Місце кримінального правопорушення одне – це місце вчинення шахрайства, а місць події, пов'язаних з цим, може бути декілька. Місце вчинення кримінального правопорушення обирається з урахуванням можливості реалізації обраного способу кримінального правопорушення, предмета посягання, особи жертви. Деякі спроби шахрайства можуть реалізовуватися в кількох місцях, не пов'язаних між собою. Може йтися й про територіальне поширення якого-небудь виду шахрайства [171, с. 430].

Матеріали слідчо-судової практики свідчать, що типовими місцями вчинення шахрайств з використанням ЕОТ є 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, як правило, належать заклади харчування, де присутня мережа Інтернет, громадські місця, де поширено розповсюдження WI-FI, місця позбавлення волі. Непоодинокі випадки, коли шахрайства, учинені з використанням ЕОТ, можуть вчинятися поза межами нашої держави, а також з тимчасово окупованих районів Донецької та Луганської областей, Автономної Республіки Крим.

Окрім того, з метою приховування IP-адрес злочинці активно використовують спеціальні програми, які не завжди дають змогу правоохоронним органам встановити місце входу ЕОТ в мережу Інтернет.

Так, перевагами VPN-з'єднання є наступні: сервери розташовані в 20 країнах світу; постійно додаються нові сервери; VPN-з'єднання захищає конфіденційність користувача і підвищує рівень безпеки; працює безкоштовно 7 годин на тиждень; забезпечує конфіденційність і захист через VPN; можливість приховати свою IP-адресу; шифрування інтернет-даних; захист персональних інтернет-даних за допомогою надійного 256-бітного

шифрування; використання будь-яких потрібних сайтів без будь-яких обмежень; надає можливість видалити банери і системи відстеження [13].

Windscribe надає 10 ГБ безкоштовного трафіку в місяць і можливість виходу в Інтернет через 25 серверів в 11 країнах. Для реєстрації не потрібні особисті дані, сервіс запитує лише логін і пароль. При бажанні можна вказати свій email, щоб отримати доступ до акаунту, якщо забудете пароль. На цю ж пошту будуть приходити повідомлення про нарахування нових лімітів трафіку [1].

Вчиненню шахрайства з використанням ЕОТ сприяють головним чином обстановка слабкого контролю за дотриманням встановленого порядку обігу контенту провайдерами, що надають інтернет-послуги, власниками вебсайтів, інтернет-мереж, соціальних мереж, недостатня захищеність комп'ютерних систем. Тут злочинці частіше використовують вже об'єктивно сформовані для них сприятливі умови, ніж спеціально створювані ними.

Підводячи підсумки, зазначимо, що місцями, де може відбуватися шахрайство, вчинене з використанням ЕОТ, як правило, є віртуальний простір, відповідно, взаємозв'язок між елементами криміналістичної характеристики розглянутого діяння передбачає, що спосіб вчинення шахрайства, його механізм обумовлюються обстановкою вчинення даного кримінального правопорушення.

1.4 Особа злочинця та особа потерпілого від шахрайств, учинених з використанням електронно-обчислювальної техніки

Особа злочинця є центральним елементом криміналістичної характеристики шахрайств, що вчиняються з використанням ЕОТ, оскільки предмет злочинного посягання, спосіб кримінального правопорушення, його слідова картина завжди пов'язані з особистісними ознаками особи злочинця

та закономірностями його поведінки. Дослідження особи злочинця оптимізує процес висунення слідчих версій і забезпечує обрання найбільш оптимальних тактичних прийомів проведення окремих СРД при розслідуванні шахрайств, що вчиняються з використанням ЕОТ. За допомогою аналізу поведінки та психології злочинця можна встановити дійсні причини й умови вчиненого кримінального правопорушення, оцінити суспільну небезпеку злочинця, здійснити правильну кримінально-правову кваліфікацію вчиненого і, як наслідок, призначити справедливе покарання.

Хоча наразі шахрайства, що вчиняються з використанням ЕОТ, набувають усе більшого розповсюдження, проте вивченню особи, яка вчиняє такі злочини, приділено недостатньо уваги, що беззаперечно ускладнює процес їх розслідування. З огляду на зазначене пріоритетним напрямом досліджень у галузі криміналістики є розробка наукових положень щодо особи злочинця як елемента криміналістичної характеристики шахрайств, що вчиняються з використанням ЕОТ.

Загальнотеоретичні положення про особу злочинця як елемент криміналістичної характеристики кримінальних правопорушень досліджували Ю. П. Аленін, Р. С. Бєлкін, П. С. Дагель, В. Ф. Єрмолович, Н. І. Клименко, В. О. Коновалова, М. В. Салтевський, В. Ю. Шепітько та інші вчені-криміналістики. Окремі кримінологічні та криміналістичні особливості злочинців, що вчиняють шахрайства з використанням ЕОТ, розглядали у своїх наукових працях Р. С. Атаманов, В. П. Сабадаш, М. М. Федотов, С. В. Шапочка та інші. Безумовно, проведені дослідження є вагомим внеском у розвиток теоретичних засад криміналістичної характеристики шахрайств, що вчиняються з використанням ЕОТ, однак в опублікованих працях зосереджувалася увага, головним чином, на загальних засадах методики розслідування цих кримінальних правопорушень. Що ж до особливостей особи, яка причетна до шахрайства з використанням ЕОТ, то вони досліджені недостатньо, що зумовлює як теоретичні дискусії, так і труднощі в процесі розслідування.

У науковій літературі висловлюються різноманітні точки зору щодо визначення сутності такого елемента криміналістичної характеристики кримінальних правопорушень, як особа злочинця. Одні вчені визначають особу злочинця як соціально-біологічну систему, властивості та ознаки якої відображаються у матеріальному середовищі та використовують для розкриття та розслідування кримінальних правопорушень (до таких властивостей відносяться: фізичні, біологічні та соціальні) [203, с. 112]. На думку інших, особа злочинця – це поняття, що виражає сутність особи, яка вчинила злочин, а до системи ознак особи злочинця включають дані демографічного характеру, деякі моральні властивості й психологічні особливості [124, с. 278–279]. Треті ж до сукупності інформації про особу злочинця, яка складає його характеристику, включають всі ті дані, які можуть визначати ефективні шляхи розшуку та викриття злочинця, і пов'язані з цим завдання розслідування [75, с. 194].

Так, В. Ю. Шепітько під особою злочинця розуміє сукупність психологічних властивостей, характерних для осіб, які вчиняють злочини [259, с. 155]. Він же наголошує на тому, що вивчення особи злочинця вимагає ґрунтовного дослідження психологічного механізму протиправної поведінки, мотивації різних видів кримінальних правопорушень, вивчення ролі та співвідношення індивідуальних психологічних і соціально-культурних чинників у формуванні особи злочинця й протиправної поведінки, а також дії на особистість стійких і ситуативних психічних станів.

Як вбачається з наведених підходів, більшість правників виокремлюють наступні елементи характеристики особи злочинця: 1) соціально-демографічні – соціальне положення, освіта, національність, сімейний стан, судимість, професія і тому подібне; 2) психологічні – світогляд, переконання, навики, звички, емоції, відчуття, темперамент тощо; 3) фізіологічні – анатомічні та функціональні ознаки, біохімічні особливості крові, слини тощо [11, с. 5].

Разом з тим вважаємо, що фізіологічні ознаки повинні бути у даному

випадку замінені на фізіологічно-розумові властивості особи, яка причетні до шахрайства з використанням ЕОТ. Пропонується наступна структура характеристики особи: а) соціально-демографічна; б) морально-психологічна; в) фізіологічно-розумова характеристика – спрямованість і характер учиненого кримінального правопорушення, наявність досвіду роботи в Інтернет-мережі, учинення кримінального правопорушення в складі групи чи організованої злочинної групи тощо [88, с. 113; 92, с. 133]. При цьому у даному випадку пропонується вивчати таку особу 1) за залишеними нею слідами за результатами використання ЕОТ та 2) в процесі розслідування кримінального правопорушення залежно від способу вчинення шахрайства.

За матеріалами узагальнення 40 кримінальних проваджень (Додаток В) встановлено, окремі риси соціально-демографічних ознак осіб, які вчиняють шахрайські дії з використанням ЕОТ, зокрема до яких можна віднести наступні. Всі шахрайства були вчинені чоловіками (100 %). Середній вік злочинця становить у 60 % від 25 до 35 років, у 32,5 % – від 18 до 25 років, понад 35 років – у 7,5 %. 70 % осіб мали незакінчену вищу або закінчену освіту, 30 % осіб – середню або середню спеціальну освіту. 64 % осіб були не одружені, 35 % – одружені. Значна кількість злочинців ніде не працювали та не навчалися (82,5 %), лише 12,5 % – навчалися, а 5 % – офіційно працювали. У 95 % осіб був відсутній попередній досвід злочинної діяльності.

Особистими характеристиками портрета такої особи є активна життєва позиція, нестандартність мислення і поведінки, обережність, уважність [179]. Також зустрічаються серед таких осіб фахівці у сфері психології, економіки, а й інколи і в різних галузях права. Деяким з них добре відомі методи роботи правоохоронних органів.

Однією з характерних особливостей шахрайства, що вчиняється з використанням ЕОТ, є, зокрема, відсутність судимості у злочинців. Зазвичай такі шахрайства вчиняються з корисливих мотивів. Хоча останнім часом широкого розповсюдження набувають шахрайства з використанням ЕОТ особами, які знаходяться в місцях позбавлення волі [210].

Що стосується психологічних ознак осіб, які вчиняють шахрайство з використанням ЕОМ, то тут необхідно зазначити, що вони досить обізнані в психології, володіють різними методами так званого заманювання осіб придбати ту чи іншу річ, при цьому вони використовують не найкращі людські якості: корисливість, пихатість, сластолюбство. Техніки виконання шахрайських прийомів різноманітні [116, с. 184].

Наприклад, у м. Запоріжжі працівники шахрайського офісу (штат співробітників – близько 100 осіб, серед яких були неповнолітні) виманювали у громадян CVV-код, номер картки, пін-код тощо. Для цього вони використовували також психологічні методи впливу та діяли за інструкцією. Крім того, щомісяця всі співробітники call-центру проходили відповідні тренінги, отримували інструкції для спілкування з клієнтами, перекладені чотирма мовами. Щодня кожен співробітник здійснював близько сотні таких дзвінків. Отриману інформацію використовували для викрадення грошей із банківських карток потерпілих [99].

За твердженням О. Л. Мусієнка, моральні властивості та психологічні особливості проявляються в моральних рисах і якостях людини: поглядах, переконаннях, оцінках, життєвих прагненнях, ціннісних орієнтаціях. Всю розмаїтість цих якостей особи можна зрештою звести до двох моментів: 1) ставлення до різних соціальних цінностей і сторін діяльності або до власності; 2) рівень, характер і соціальна значущість її потреб [156].

Ю. М. Піцик, здійснюючи дослідження особистості кіберзлочинця, який вчиняє злочини проти власності, зазначає, що у порівнянні з традиційними видами шахрайства інтернет-шахрайство є досить «молодим» видом кримінального правопорушення. Згідно зі статистичними даними, більшість кіберзлочинів проти власності (79 %) – це шахрайства, учинені чоловіками (94 %). Такі злочини вчиняють здебільшого особи, які офіційно не перебувають у шлюбі та не мають дітей. Кількість неодружених осіб становить 70 %, одружених – 30 %. Згідно з даними судової практики, 51 % осіб, які вчинили кіберзлочини, не мають постійного місця роботи, такі особи

вчиняють зазвичай шахрайства. Серед решти 49 % більшість становлять менеджери нижчої та середньої ланок, рідше – посадові особи та програмісти. Якщо середній вік шахрая в матеріальному світі становить 26–39 років, то середній вік кібершахрая – від 18 до 40 років. Соціальне становище в суспільстві – від студента до співробітника державної установи або фірми [173, с. 106].

Погоджуючись з Л. М. Прудкою, зазначимо, що значна кількість шахрайств, що вчиняються з використанням ЕОТ, має специфічну ціннісну орієнтацію шахрая, а саме його відношення до жертви як до неживого об'єкта. Людина для нього насамперед – це можливе джерело власних матеріальних благ. Внутрішній світ жертви, її переживання, страждання у разі позбавлення матеріальних цінностей для злочинця не мають значення.

У шахрайських посяганнях на перший план виступає яскраво виражений корисливий мотив. Проте, окрім користі, мотивами шахрайської діяльності можуть бути: самоствердження, приховане прагнення до влади. Залежно від домінування того або іншого мотиву у разі вчинення кримінального правопорушення кримінального правопорушення Л. М. Прудка пропонує поділити шахраїв, що використовують маніпуляцію свідомістю і поведінкою жертв, на такі групи:

1) шахраї з провідним корисливим мотивом, раціональним підходом до способу вчинення шахрайства, підготовкою до його вчинення і усвідомленням усіх наслідків злочинної діяльності;

2) шахраї з провідним ігровим мотивом (шахрай – гедоніст, що отримує задоволення від процесу злочинної діяльності);

3) шахраї з ведучим ситуативно виниклим мотивом, під впливом сприятливих (з точки зору реалізації злочинного задуму) обставин;

4) шахраї з провідним мотивом, що виник під впливом групового тиску [185, с. 32].

Серед шахраїв, які орудують через мережу Інтернет, найбільше зустрічаються злочинці з корисливими та ігровими мотивами. В основі

мотивації корисливих злочинців, зокрема шахраїв, лежать гіпертрофовані (завищені) матеріальні потреби. Корисливі злочинці здебільшого не бачать цінностей поза матеріальною сферою, основною їхньою властивістю є неконтрольоване прагнення до матеріального збагачення [185, с. 32].

Що стосується фізіологічно-розумової характеристики шахраїв, то в більшості випадків ними є особи, які володіють навичками використання комп'ютерної техніки та інших електронних засобів, вмінням працювати в мережі Інтернет, та в окремих випадках, вузьку спеціалізацію, оскільки виконати певні дії з ЕОТ з метою вчинення шахрайства може обмежене коло осіб: а) аматори, тобто ті, що діють самостійно, в домашніх умовах і вільний від роботи час, б) високоосвічені спеціалісти, які діють у складі організованих злочинних груп. Необхідно підкреслити, що до складу такої групи обов'язково входить один або кілька учасників, які є програмістами або хоча б володіють знаннями та навичками в галузі комп'ютерних інформаційних технологій [52, с. 181].

У науковій літературі наголошується, що при вивченні особи шахрая варто звернути увагу на роль навичок і звичок, що властиві кожній людині [173]. При розслідуванні шахрайства, що вчиняється з використанням ЕОТ, вивчення цих якостей має велике значення для розшуку, виявлення злочинця, тому що нерідко саме навички і звички шахрая впливають на обирані ним спосіб і механізм вчинення кримінального правопорушення. Погляди вчених на місце навичок і звичок у системі криміналістичної характеристики кримінальних правопорушень рівні. Так, серед ознак, що мають самостійне криміналістичне значення, С. П. Митричев називає професійні та злочинні навички злочинця. Знання звичок і навичок шахрая відіграє певну роль через те, що ці якості людини індивідуалізують її протиправне діяння, й чим специфічніше та складніше навичка, тим більше часу і зусиль потрібно на її освоєння, тим вище її криміналістична значущість [150].

Злочинець особисто не контактує із своєю жертвою, а здійснює свої

злочинні дії шляхом телефонних розмов, надсилання SMS-повідомлень або через інтернет-листування [62]. Типологія особи диференціюється на відмінностях характеру антигромадської її спрямованості та ціннісних орієнтаціях, до яких належить негативне ставлення до важливих благ людської особистості [156].

Виходячи із загальних положень криміналістичної характеристики, результатів кримінологічних досліджень, необхідно виокремити ті властивості особи, яка вчиняє шахрайські дії з використанням ЕОТ, вивчення яких дозволяє розробити рекомендації для обрання правильного напряму розслідування, забезпечення найбільш ефективної тактичної лінії у провадженні слідчих (розшукових) дій; встановити, які риси цієї особи повинні враховуватися при виявленні цього виду кримінального правопорушення та їхньому розкритті. Особа шахрая, який вчиняє кримінальне правопорушення з використанням ЕОТ, характеризується специфічним комплексом ознак. Більшість злочинців мають сильний дар уяви, вони використовують вплив і вміння переконувати людей [122, с. 520]. Щодо якостей особистості злочинця, варто встановити те, що в деяких випадках однією з важливих якостей особистості інтернет-шахрая є наявність організаторських здібностей, оскільки деякі види інтернет-шахрайства є технічно складними в плані виконання, а тому у їх вчиненні можуть брати участь кілька людей.

Для прикладу, з метою вчинення фітингу було створено угруповання у складі чотирьох осіб, яке заволоділо грошовими коштами держателів платіжних карт шляхом несанкціонованого їх списання через системи on-line платежів [48].

М. І. Омельяненко та О. А. Севідов залежно від прихильності осіб використовувати певні способи для заволодіння майном шляхом шахрайства, учиненого з використанням ЕОТ, пропонують наступну класифікацію таких осіб.

Кардери. Спеціалізуються на махінаціях з пластиковими картками, оплачуючи свої витрати з чужих кредитних карток. Типова процедура кардинга полягає в копіюванні інформації, що міститься на магнітній смузі кредитної картки (дамп) і виробництві фальшивої картки-«фантома» з нанесенням на неї скопійованого дампа або одержанням індивідуального пін-коду від власника реальної карти, наприклад, методами соціальної інженерії. Ці особи також займаються викраденням номерів кредитних карт з подальшим отриманням доступу до рахунків осіб, чиї номери і коди карт були викрадені. Цією групою використовуються різні методи, від елементарного підглядання коду карти з наступною крадіжкою самої карти до крадіжки номерів з пам'яті ЕОТ, створення підставних банкоматів та інтернет-магазинів [210].

Кіберкруки. 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. Використовують комп'ютерні системи та мережі для викрадення грошових коштів, отримання цінної фінансової інформації. Популярним предметом посягання є кредитна інформація, інформаційні бази даних правоохоронних органів та інших державних і комерційних структур. Тому, нерідко отриману інформацію вони продають іншим особам [164].

Фішери. Їх метою є заволодіння обманним шляхом персональними даними клієнтів онлайн-аукціонів, інтернет-магазинів, сервісів грошових переказів та іншої конфіденційної інформації. Постійно удосконалюються шахраями різні «схеми», які спрямовані, в основному, на занадто довірливих або неуважних користувачів, які самі (добровільно) надають конфіденційну інформацію, коли їх просять повторити введення пароля, повідомити номер рахунку та пароль для реєстрації покупки або грошового переказу, зареєструватися на лже-сайті інтернет-магазину тощо. Фішери створюють підставні сайти (наприклад, копії сторінки банку), заходячи на який власник

карти, бажаючи перевірити свій рахунок, вводить конфіденційні дані, які згодом використовуються зловмисником [164].

Спамери. Займаються масовою (більш ніж 5-ти адресатам) розсилкою (часто анонімних) оголошень засобами електронних комунікацій, насамперед – по електронній пошті чи в соціальних мережах. Як правило, діють в інтересах третіх осіб за матеріальну вигоду [164].

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. Усвідомлення цінності доменів постійно зростає, а слідом зростає і їхня ціна [164].

Фрікери. 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. Їх злочинна діяльність спрямована на отримання кодів доступу, розкрадання телефонних карток і номерів доступу з метою перенести оплату на рахунок іншого абонента [164].

Згідно зі статистичними даними, більшість кіберзлочинів проти власності (79 %) – це шахрайства, учинені чоловіками (94 %). Такі злочини вчиняють здебільшого особи, які офіційно не перебувають у шлюбі та не мають дітей. Кількість неодружених осіб становить 70 %, одружених – 30 %. Згідно з даними судової практики, 51 % осіб, які вчинили кіберзлочини, не мають постійного місця роботи, такі особи вчиняють зазвичай шахрайства. Серед решти 49 % більшість становлять менеджери нижчої та середньої ланок, рідше – посадові особи та програмісти. Якщо середній вік шахрая в матеріальному світі становить 26–39 років, то середній вік кібершахрая – від 18 до 40 років. Соціальне становище в суспільстві – від студента до співробітника державної установи або фірми [173, с. 106].

Поняття потерпілого міститься у ч. 1 ст. 49 КПК України: «Потерпілим визнається особа, якій злочином заподіяно моральну, фізичну або майнову шкоду» [132]. Особа потерпілого є суттєвим елементом криміналістичної характеристики досліджуваної категорії кримінальних правопорушень. Відомості про особу жертви безпосереднім чином «проливають світло» на інші обставини події кримінального правопорушення.

Зважаючи на специфіку досліджуваного нами виду шахрайства, доречно зазначити, що потерпілим може бути будь-яка особа: громадянин України, іноземець чи особа без громадянства, що постійно проживає на території України, та повинен мати повну цивільну дієздатність.

У контексті дослідження особи потерпілого від шахрайства представляється слушним встановлення відношення самого потерпілого до факту обману відносно нього або його ставлення до того, що в результаті висловлення власної довіри до певної особи (осіб) він був ошуканий [54].

Специфіка предмета шахрайства обумовлена закономірним зв’язком з особою потерпілого. У багатьох випадках при вчиненні шахрайства, особливо під час його підготовки, злочинець, оцінюючи реальну ситуацію, в якій йому доведеться діяти або в якій він уже діє, не може не враховувати вік, стать, фізичну силу, інтелектуальні можливості та інші індивідуальні якості потерпілого. Зв’язок «злочинець – потерпілий» виникає як наслідок розвитку злочинної події та дій особи, яка вчинила злочин, і її взаємодії з потерпілим. Акт злочинного посягання перетворює наявний до цього зв’язок згаданих осіб (який мав особистий, побутовий або інший характер) у зв’язок кримінальний. У разі якщо злочинець і потерпілий до посягання не зустрічалися, не були знайомі, в основі розвитку зв’язку лежить лише факт учинення кримінального правопорушення [104, с. 78].

Поведінка потерпілого може виявлятися у різних проявах: від повної віктимності, уразливості до впливу шахрая, нейтрального ставлення до останнього або активної протидії йому. Саме тому, що часто потерпілі самі провокують вчинення відносно них обманних дій, і відбувається подія

кримінального правопорушення [54, с. 76].

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. [55].

Постраждати від шахрайства може практично кожен. Але існують певні характерні соціально-психологічні властивості особистості або їх комплекси, які можуть спричиняти віктимізацію особи стосовно шахрайства. Деякі дослідники, зокрема, зазначають, що підвищена віктимність у зв'язку з психологічними особливостями здебільшого притаманна саме потерпілим від шахрайства [134, с. 135].

Природа вчинення шахрайства з використанням ЕОТ передбачає тривалий вербальний або конклюдентний контакт, або контакт в комплексі між потерпілим і злочинцем. Результатом такого контакту є введення першого в оману або маніпулювання його довірою. Тому вивчення зв’язку «потерпілий – злочинець» необхідне для побудови повної криміналістичної характеристики кримінального правопорушення, обрання тактики проведення окремих слідчих дій [55].

Залежно від наявності й впливу різних відносин, що існували або утворилися між злочинцем і потерпілим до вчинення кримінального правопорушення, проводиться розділення зв’язку за обставинами його утворення. 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. 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 [157, с. 83–85].

Ураховуючи, що особистість жертви шахрайства становить інтерес, насамперед, з точки зору її віктимного потенціалу стосовно цього кримінального правопорушення, в її соціально-психологічному дослідженні, окрім вже названих, можна визначити певні додаткові орієнтири. Це, зокрема, соціальнопсихологічні чинники зниження критичності, обачності особи. Саме необачна поведінка властива переважній більшості жертв шахрайства. При цьому необачність потрібно розглядати не лише як сутнісну (сталу) властивість особистості, але і як одну з ознак поведінки у конкретній ситуації, яка залежить, з одного боку, від соціального досвіду особи, її поінформованості, звичок, інших особистісних властивостей, а з іншого – від впливу елементів зовнішнього середовища, у якому потенційна жертва опиняється у конкретний момент часу [176, с. 164–169].

Підводячи підсумки до підрозділу зазначимо, що дослідження особи злочинця, який вчиняє шахрайства в мережі Інтернет, є важливим елементом криміналістичної характеристики, оскільки її вивчення дасть змогу визначити основні напрями для розшуку та встановлення злочинця.

Шахрайство – це складова елементів трикутника: мотив, можливості, раціональність. Підґрунтям шахрайства є емоційний вплив на жертв. «Професійні» звички та почерк злочинців виражені певними способами, методами, прийомами вчинення кримінальних правопорушень. Залишені на місці кримінального правопорушення сліди засвідчують особливості його соціально-психологічного портрета: досвід, професія, вік, стать, знання тощо.

Формування банку типових моделей різних категорій злочинців дасть змогу оптимізувати процес виявлення кола осіб, серед яких найбільш вірогідний пошук злочинця [162, с. 181]. Зібрані в процесі розслідування відомості про особу злочинця, його кримінальну поведінку та злочинні дії створюють фактичну базу прийняття обґрунтованих правових рішень для його переслідування [4, с. 55].

Висновки до розділу 1

Не дивлячись на значну кількість наукових праць, присвячених проблемам розслідування кримінальних правопорушень, учинених з використанням ЕОТ (А. І. Анапольська, С. В. Головкін, Н. Ю. Кириленко, С. М. Князєв, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, О. М. Стрільців, С. С. Чернявський та інші) на сьогодні залишаються недостатньо дослідженими в українській криміналістиці саме шахрайства, учинені з ЕОТ, монографічні дослідження за вказаним напрямом не проводились. Лише опубліковано окремі статті та методичні рекомендації, присвячені виявленню та розслідуванню шахрайств, що вчиняються з використанням ЕОТ.

Наголошено на необхідності узагальнення і впорядкування наявних методичних рекомендацій щодо розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки, з метою формування комплексної криміналістичної методики. Об’єднані в єдиній класифікаційній групі ідеї й теоретичні положення стають цілісною теоретичною концепцією, в основі якої – характеристика різних видів кримінальних правопорушень, урахування якої дозволяє об’єднати окремі рекомендації в єдину методику.

Також потребують подальшого дослідження можливості виявлення та встановлення місця, з якого здійснювалось використання ЕОТ, а також доказування причетності певних осіб до користування ЕОТ з метою вчинення

шахрайства. Виходячи зі стану наукового дослідження проблеми розслідування шахрайств, учинених з використанням ЕОТ, обґрунтовано необхідність здійснення подальших досліджень цієї проблематики.

Надаючи криміналістичну характеристику шахрайств, учинених з використанням ЕОТ, констатовано, що дані про спосіб учинення такого кримінального правопорушення є основним підґрунтям для висунення і перевірки слідчих версій щодо особи злочинця та дозволяють встановити слідову картину кримінального правопорушення, оскільки для конкретних способів учинення чи приховування кримінального правопорушення характерні певні види слідів і механізми їх утворення.

За результатами проведеного дослідження встановлено способи вчинення шахрайств з використанням ЕОТ, які поділені залежно від: а) періодичності вчинення кримінального правопорушення; б) сфери застосування; в) кількості задіяних до вчинення шахрайства осіб; г) предмета посягання; д) виду ЕОТ, яка використовувалась; е) інформаційної підтримки; є) характеру «стосунків», що виникають між потерпілим і злочинцем; ж) місця створення та місця реєстрації IP-адреси ЕОТ; з) способів введення в оману або зловживання довірою; і) характеру подання відомостей.

Також визначено найбільш поширені в державі способи шахрайств, учинених з використанням ЕОТ, які умовно можна диференціювати на такі: 1) заволодіння інформацією у власників платіжних карток про їх реквізити та іншу конфіденційну інформацію й подальше заволодіння коштами з банківського рахунку потерпілого; 2) створення Інтернет-аукціонів шляхом надання недостовірних даних і пропозицій щодо продажу неіснуючих товарів; 3) заволодіння майном шляхом створення та діяльності фіктивних фінансових бірж; 4) заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій; 5) заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину, а також інші способи.

Визначено, що предметом шахрайств, учинених за допомогою ЕОТ, можуть бути: майно (рухоме, нерухоме); право на майно; кошти; інформація.

Зазначено, що залежно від способів учинення шахрайств з використанням ЕОТ формуються три групи типових слідів: матеріальні (речові), цифрові та віртуальні. Так, до матеріальних можна віднести сліди пальців рук і біологічні сліди, що залишаються на ЕОТ та інших засобах, які використовувались під час вчинення шахрайства (на клавіатурі, дисководах, джерелах безперебійного живлення, принтері, робочому місті тощо), а також на предметах, отриманих в результаті шахрайства. До цифрових слідів належать сліди, що залишені в ЕОТ під час створення певного контенту та користуванням інтернет-мережею. Віртуальні сліди залишаються у пам’яті свідків чи осіб, які вчинили шахрайство чи причетні до нього.

Обстановка вчинення шахрайств з використанням ЕОТ засвідчує, що такі злочини вчиняються у віртуальному середовищі, де, як правило, залишаються лише інформаційні сліди.

Проведене вивчення результатів кримінальних проваджень за фактом вчинення шахрайств з використанням ЕОТ дозволило визначити характерні ознаки особи, яка причетна до цього кримінального правопорушення. Це особи переважно чоловічої статі (100 % вивчених кримінальних проваджень); середній вік складає від 25 до 35 років (60 %), від 18 до 25 років – 32,5 %, понад 35 років – 7,5 %. Як правило, такі особи мають незакінчену вищу освіту (45 %), вищу – 25 %, середню – 17,5 %, середню спеціальну – 12,5 %. Більшість з таких осіб не одружені (65 %), не працюють та не навчаються – 82,5 %, навчаються – 12,5 %, офіційно працевлаштовані – 5 %, при цьому тільки 5 % мали попередній досвід злочинної діяльності. Специфікою потерпілого є те, що такою особою може бути практично кожен.

РОЗДІЛ 2
ПОЧАТКОВИЙ ЕТАП РОЗСЛІДУВАННЯ ШАХРАЙСТВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

2.1. Обставини, які підлягають встановленню під час розслідування шахрайств, учинених з використання електронно-обчислювальної техніки

Упродовж тривалого часу існування криміналістика накопичила чималі знання, що стосуються методики розслідування кримінальних правопорушень взагалі та кримінальних правопорушень проти власності зокрема. Проте не дивлячись на поширення такого виду шахрайства, що вчиняється з використанням ЕОТ, на сьогодні відчувається недостатньо розробленою методика розслідування цього кримінального правопорушення, що засвідчує аналіз проведеного анкетування слідчих (Додаток Б).

Чинний КПК України [132] серед завдань кримінального провадження називає повне розслідування та судовий розгляд. Таке положення розвивається нормою ст. 94 КПК України, відповідно до якої слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв’язку для прийняття відповідного процесуального рішення [132]. В науці криміналістиці наявні різні підходи до об’єднувальної назви таких обставин – обставин, що підлягають з’ясуванню, встановленню або доказуванню під час розслідування кримінального правопорушення.

Наразі відсутня єдина позиція науковців щодо терміна, який визначає

обставини, що підлягають з’ясуванню (доказуванню, встановленню) під час розслідування кримінального правопорушення, зокрема шахрайства, учиненого з використанням ЕОТ.

Так, одні науковці під предметом доказування розуміють діяльність органів розслідування, прокурора і суду, а також інших учасників процесу, яка здійснюється у встановлених законом процесуальних формах і спрямована на збирання, закріплення, перевірку й оцінку фактичних даних (доказів), необхідних для встановлення істини у кримінальній справі [163, с. 75].

С. М. Стахівський вказує на різні погляди науковців на визначення поняття кримінально-процесуального доказування: від видалення оцінки доказів за межі цього процесу до включення до нього криміналістичних категорій (слідчих версій) [221, с. 19]. При цьому ним стверджується, що це передбачена законом діяльність суб’єктів кримінального процесу по збиранню (формуванню), перевірці й оцінці доказів та їх процесуальних джерел, прийнятті на цій основі певних процесуальних рішень і наведенню аргументів для їх обґрунтування (мотивації) [221, с. 21].

Обставини, які підлягають доказуванню у кримінальному провадженні, визначено у ч. 1 ст. 91 КПК України і становлять: 1) подію кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення); 2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форму вини, мотив і мету 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 [132].

Вказані обставини, що відображені в нормах чинного КПК України, є визначальними, базовими для всіх злочинних діянь без винятку, а також для криміналістичної методики розслідування, тому мають неабияке значення.

На відміну від термінологічного апарату кримінального процесу, у науці криміналістиці послуговуються іншим терміном, а саме «обставини, що підлягають встановленню», які, відповідно до структури окремих криміналістичних методик, є окремим їх елементом [255, с. 37–38], їх розглядають за деякими елементами складу кримінального правопорушення [180].

Це видається логічним, оскільки коло обставин, пов'язаних з доказуванням події кримінального правопорушення, винуватості особи в його вчиненні, форми вини, мети і мотивів, деталізується і залежить від того, як сформульовано склад кримінального правопорушення у відповідній нормі кримінального закону. З'ясування цих обставин має послідовно давати відповіді на класичне запитання юриспруденції: «Що, де, коли, ким, яким чином?..» [233, с. 48].

Так, В. А. Журавель оперує терміном «обставини, що підлягають з'ясуванню», які, на його думку, зумовлені трьома чинниками: предметом доказування (ст. 91 чинного КПК України), кримінально-правовою та криміналістичною характеристикою певного різновиду злочинного

посягання. При цьому обставини, що підлягають доказуванню, як структурний елемент окремої криміналістичної методики є значно ширшими, ніж предмет доказування в розумінні КПК України [77, с. 13]. Це він пов'язує з тим, що встановлення обставин, які підлягають з'ясуванню, закон відносить до початку досудового розслідування. Відповідно до ст. 214 КПК України слідчий, дізнавач, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до ЄРДР, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з ЄРДР. Частина 2 цієї статті визначає, що досудове розслідування розпочинається з моменту внесення відомостей до ЄРДР [132]. При цьому ч. 3 ст. 214 КПК України передбачається у невідкладних випадках до внесення відомостей до ЄРДР може бути проведений огляд місця події (відомості вносяться невідкладно після завершення огляду). Для з'ясування обставин вчинення кримінального правопорушення до внесення відомостей до ЄРДР може бути:

1) відібрано пояснення;

2) проведено медичне освідування;

3) отримано висновок спеціаліста і знято показання технічних приладів і технічних засобів, що мають функції фотозйомки і відеозапису, чи засобів фотозйомки, відеозапису;

4) вилучено знаряддя і засоби вчинення кримінального правопорушення, речі й документи, що є безпосереднім предметом кримінального правопорушення, або які виявлені під час затримання особи, особистого огляду або огляду речей [132].

Таким чином, на етапі попереднього розслідування необхідно встановити події й факти, які можуть опосередковано свідчити про вчинення шахрайства з використанням ЕОТ та базуються на всебічному з'ясуванні всіх

обставин, які характеризують об'єктивні ознаки складу кримінального правопорушення, що необхідні для його правильної кваліфікації виходячи з попереднього вивчення залишених слідів як матеріальних (зміни у світі речей), так і ідеальних (спогади людей).

Ми поділяємо думку авторів, що відстоюють «широке» тлумачення предмета доказування, змістом якого є сукупність обставин, сформованих з норм кримінального і кримінального процесуального права, що необхідно встановити за конкретними категоріями кримінальних проваджень для реалізації завдань кримінального судочинства. Решту обставин безпосередньо не зазначено в законі, проте вони сприяють доказуванню, утворюють обставини, що підлягають встановленню та належать до категорії криміналістично значущих [142, с. 65–66].

Таким чином, до обставин, які підлягають встановленню, належать обставини, що підлягають доказуванню, тобто ті, які становлять предмет доказування, а також проміжні факти й обставини, корті необхідно дослідити, але які не охоплені предметом доказування, визначеному КПК України, та залишаються поза його межами [29, с. 22].

Стосовно цього, як вбачається, комплекс елементів криміналістичної характеристики має велику пізнавальну цінність, тому що поряд з індивідуальною значимістю окремих елементів дає можливість використовувати залежності між елементами (нерідко в криміналістичній літературі іменовані закономірними зв'язками), які створюють передумови для визначення особи злочинця, шляхів формування слідчих версій і визначення напряму розслідування.

Отже, з огляду на окреслене обставини, що підлягають встановленню на попередньому етапі досудового розслідування кримінального провадження, пов'язаного з шахрайством, учиненого з використанням ЕОТ, на нашу думку, доцільно об'єднати у наступні групи:

1) обставини, що стосуються самої події кримінального правопорушення. До цієї категорії потрібно зараховувати відомості про

подію кримінального правопорушення.

Подія кримінального правопорушення відбувається в певних умовах, місці та часі. Сукупність цих умов у криміналістиці називають «обстановка кримінального правопорушення». Обстановка вчинення кримінального правопорушення має важливе значення для практичної, дослідницької діяльності криміналістичної спрямованості та визначає коло обставин, що підлягають доказуванню.

Установлення способу вчинення шахрайства створює передумови для з'ясування форми вини під час вирішення питання про притягнення особи до кримінальної відповідальності за відповідною статтею КК України. Суть способу у цьому випадку полягає у незаконному оберненні чужого майна на свою користь чи користь третіх осіб з використанням при цьому ЕОТ.

Відомості про знаряддя (засоби) вчинення кримінального правопорушення, зокрема, яким чином використовувалася Інтернет-мережа та засоби телекомунікаційного зв'язку під час вчинення шахрайства з використанням ЕОТ, а також відомості про сліди кримінального правопорушення (механізм слідоутворення).

Відомості про час вчинення шахрайства та його місце. У криміналістиці прийнято вважати, що місце кримінального правопорушення охоплює всі ділянки простору, на яких виконують кожен з елементів способу, що використовував винний.

Одночасно встановлюються та перевіряються наступні обставини, які стосуються самої події кримінального правопорушення, а саме: 1) чи був факт вчинення шахрайства; 2) було вчинене шахрайство чи мало місце інсценування кримінального правопорушення; 3) чи використовувалось під час шахрайства ЕОТ; 4) час і місце вчинення шахрайства; 5) способи вчинення шахрайства та які дії здійснював злочинець для підготовки та приховування кримінального правопорушення; 6) які сайти, вебпортал чи соціальні мережі використовувалися для вчинення шахрайства; 7) яким чином були переведені (надані) кошти злочинцю; 8) хто був очевидцем

вчинення шахрайства;

2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення. Винуватість є однією з обставин, які підлягають доказуванню в кримінальному провадженні (п. 2 ч. 1 ст. 91 КПК України) [132]. Відповідно до змісту диспозиції ст. 62 Конституції України [112] та ч. 2 ст. 17 КПК України [132] доведення винуватості особи є обов'язком сторони обвинувачення – слідчого органу досудового розслідування, керівника органу досудового розслідування, прокурора й оперативних підрозділів.

Згідно зі ст. 23 КК України вина – психічне ставлення особи до вчинюваної дії чи бездіяльності, передбачених КК України, та її наслідків, виражених у формі умислу або необережності [131]. У кримінальному ж процесі, залишаючись елементом складу кримінального правопорушення, вона постає в іншому аспекті – як винність обвинуваченого, її має бути засвідчено, обґрунтовано доказами [151]. Основним змістом кримінально-процесуального за своїм характером поняття «винуватість» є констатація того, що саме ця особа вчинила відповідне діяння, яке містить склад конкретного кримінального правопорушення [72, с. 41].

Ми поділяємо думку А. О. Ляша, згідно з якою зміст «винуватості» у кримінальному процесі можна визначити через наявність таких структурних елементів: 1) фізична осудна особа, яка вчинила протиправне діяння; 2) досягнення нею віку кримінальної відповідальності на час учинення кримінального правопорушення; 3) наявність у цієї особи передбаченої кримінальним законом форми вини та її видів [143, с. 74]. Основою визнання винуватості доведеною є внутрішнє переконання суб'єкта доказування про достатність і достовірність доказів того, що кримінально протиправне діяння вчинила саме та особа, щодо якої здійснюють переслідування.

Корисну інформацію під час дослідження особи злочинця дають мотив і мета вчинення суб'єктом шахрайства. Мотив – усвідомлена підстава,

обумовлене бажання досягти конкретно визначеної мети. Він тісно пов’язаний з виною, але не збігається з нею. Впливаючи на свідомість людини, мотив формує спрямованість волі, зумовлює характер її дій [60, с. 84]. Мотивом під час вчинення шахрайства з використанням ЕОТ, як правило, виступає користь. Мотив дає змогу відмежовувати вказане кримінальне правопорушення від інших, суміжних, або засвідчує відсутність суспільної небезпеки діяння, а також є обставиною, що обтяжує або пом’якшує покарання. З’ясування мотиву шахрайства з використанням ЕОТ є одним з головних завдань під час розслідування кримінальних правопорушень цієї категорії. Дані про мотиви й мету вчинення мають бути використані під час формулювання слідчих версій стосовно суб’єкта та суб’єктивної сторони протиправної дії, організації пошуку злочинця, вибору тактичних прийомів, у процесі проведення певних СРД та НСРД.

З’ясування мотиву кримінального правопорушення також потребує з’ясування такої складової суб’єктивної сторони кримінального правопорушення, як мета, що підлягає обов’язковому доказуванню в кримінальному провадженні та передбачена ст. 91 КПК України [132] як окремий елемент предмета доказування. Лише в комплексі мотив і мета можуть сформувати повне уявлення про спрямованість поведінки особи, яка вчинила шахрайство з використанням ЕОТ. Мотив і мета кримінального правопорушення тісно пов’язані між собою. Не довівши мотив кримінального правопорушення, неможливо встановити його мету, і навпаки [79, с. 101].

Крім того, мотив і мета вчинення кримінального правопорушення пов’язані з соціально-психологічною та криміналістичною характеристиками особи злочинця. Вони належать до групи суб’єктивних чинників і в такий спосіб впливають на вибір засобів і прийомів досягнення цілей. А отже, визначають характер основних дій злочинця, спосіб учинення кримінального правопорушення, вольових дій людини і є головним аспектом будь-якого злочинного посягання;

3) вид і розмір шкоди, завданої кримінальним правопорушенням, а саме відомості про предмет злочинного посягання (його кількісні та якісні характеристики), яким виступатиме майно, яке було ввірене винному чи було в його віданні, тобто воно знаходилось у правомірному володінні винного, який був наділений правомочністю з розпорядження, управління, доставки або зберігання такого майна [16].

Предметом кримінального правопорушення переважно вважають будь-які речі матеріального світу, з певними властивостями яких закон пов'язує наявність у діях особи ознак складу кримінального правопорушення [232, с. 40, 56]. Серед дослідників переважає думка, що предмет кримінального правопорушення обов'язково фігурує в законодавчому визначенні певного кримінального правопорушення або однозначно «витікає» з такого визначення. Інші автори обстоюють ширше тлумачення предмета кримінального правопорушення. Зокрема, предметом кримінального правопорушення вони вважають фізичних осіб і їхні дії, юридичних осіб, а також речі та процеси, які слугують умовою існування або формою вираження суспільних відносин [22, с. 123].

Така правомочність може обумовлюватись службовими обов'язками, договірними відносинами або спеціальним дорученням. Крім того, предметом кримінального правопорушення може бути і майно, яке безпосередньо не було ввірене винному чи не перебувало в його віданні, а це майно, щодо якого в силу своєї посади (постійно чи тимчасово) винний наділений правомочністю управління чи розпорядження майном через інших осіб. Тобто він має певні владні повноваження щодо впливу на осіб, яким це майно ввірено чи перебуває у їх віданні [16].

Доказувати вид, розмір і характер шкоди, завданої кримінальним правопорушенням, необхідно для визначення розміру стягнення за цивільним позовом й обсягу майна, на яке можливе накладення арешту. Також вид і розмір шкоди можуть бути обставинами, від яких залежить кваліфікація кримінального правопорушення, визначення ступеня вини та розміру

покарання підсудного. Для визначення характеру й ступеня суспільної небезпечності кримінального правопорушення необхідно встановити розмір шкоди, що іноді має вирішальне значення для визнання діяння злочинним і встановлення тяжкості кримінального правопорушення [19, с. 79]. Вид і розмір шкоди встановлюють у кожному кримінальному провадженні незалежно від того, чи впливає така шкода на кваліфікацію діяння.

Встановлення наявності причинного зв'язку між кримінальним правопорушенням і шкодою, тобто те, що шкоду завдано саме внаслідок вчинення кримінального правопорушення, має важливе практичне значення, оскільки за його відсутності немає підстав для позову. Протиправна поведінка особи тільки тоді є причиною шкоди, коли вона безпосередньо пов'язана з цією шкодою. Наявність непрямого (опосередкованого) зв'язку між протиправною поведінкою особи та шкодою означає, що така поведінка знаходиться за межами конкретного випадку, а отже, і за межами юридично значущого причинного зв'язку [40, с. 7].

Відповідно до п. 3 ч. 1 ст. 91 КПК України [132] у кримінальному провадженні підлягає доказуванню також розмір процесуальних витрат. Судові витрати в кримінальному провадженні охоплюють витрати: на правову допомогу (ст. 120 КПК України); пов'язані з прибуттям до місця досудового розслідування або судового провадження (ст. 121 КПК України); пов'язані із залученням потерпілих, свідків, спеціалістів, перекладачів та експертів (ст. 122 КПК України); пов'язані зі зберіганням і пересиланням речей і документів (ст. 123 КПК України) [132];

4) відомості, що характеризують особу підозрюваного.

У межах встановлення обставин, що характеризують особу підозрюваного, інтерес становить інформація, яка безпосередньо не пов'язана з учиненим кримінальним правопорушенням. До таких відомостей належать дані про: вік особи, стан її здоров'я, поведінку, взаємини, колишні судимості тощо. До суб'єктивних чинників, які визначають такий структурний елемент криміналістичної характеристики, як «особа злочинця»,

потрібно віднести: наявність у злочинців попереднього злочинного досвіду, зокрема й знання ЕОТ, сфери комунікаційного зв'язку, конкретних способів учинення, приховування слідів у мережі Інтернет, індивідуальні властивості особи злочинця тощо;

5) обставини, які пом'якшують або обтяжують покарання, відображено в ст. ст. 66 і 67 КК України [132]. Під час призначення покарання обставинами, які його пом'якшують, визнають: з'явлення із зізнанням, щире каяття або активне сприяння розкриттю кримінального правопорушення; добровільне відшкодування заподіяної шкоди або її усунення; надання медичної чи іншої допомоги потерпілому безпосередньо після вчинення кримінального правопорушення; учинення кримінального правопорушення неповнолітнім; учинення кримінального правопорушення жінкою в стані вагітності; учинення кримінального правопорушення внаслідок збігу тяжких особистих, сімейних чи інших обставин; учинення кримінального правопорушення під впливом погрози, примусу або через матеріальну, службову чи іншу залежність; учинення кримінального правопорушення під впливом сильного душевного хвилювання, зумовленого неправомірними або аморальними діями потерпілого; учинення кримінального правопорушення з перевищенням меж крайньої необхідності; виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи чи злочинної організації, поєднане з учиненням кримінального правопорушення у випадках, передбачених КК України [131]. У разі якщо слідчий під час досудового розслідування встановить обставини, які, на його думку, можуть бути розглянуті судом як пом'якшуючі, він повинен зазначити їх в обвинувальному акті;

6) звільнення від кримінальної відповідальності – це здійснювана відповідно до вимог кримінального та кримінально-процесуального законів відмова держави в особі суду від застосування щодо особи, яка вчинила злочин, обмежень її певних прав і свобод, передбачених КК України, що не тягне за собою кримінально-правових наслідків [21, с. 58]. Для правильного

трактування сутності обставин, за наявності яких законодавець або взагалі виключає злочинність і караність діяння (тим самим особу не притягують), або вважає недоцільним притягнення особи до кримінальної відповідальності (тобто особа звільняється від кримінальної відповідальності), найважливіше значення має розгляд ознак кримінального правопорушення, які й визначають його поняття [74, с. 29].

Кримінальний закон встановлює, що звільнення від кримінальної відповідальності здійснює виключно суд. У всіх випадках звільнення від кримінальної відповідальності, слушно зазначає Ю. М. Грошевий, суд повинен достовірно доказати наявність у діях підсудного всіх елементів складу кримінального правопорушення [64, с. 26];

7) законодавчо визначено (п. 7 ч. 1 ст. 91 КПК України) [132], що в кримінальному провадженні можуть також встановлювати обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру. Перелік таких підстав міститься в КК України. Так, зокрема, в ст. 96^3 КК України визначено, що однією з підстав для застосування до юридичної особи заходів кримінально-правового характеру є вчинення її вповноваженою особою від імені юридичної особи будь-якого кримінального правопорушення.

Виключає можливість застосування до юридичної особи будь-якого заходу кримінально-правового характеру також і закриття кримінального провадження щодо вповноваженої особи юридичної особи на стадії судового слідства (ст. ст. 45–48, ч. 6 ст. 258, ч. 2 ст. 258^3, ч. 4 ст. 258^5 КК України, п. 1 ч. 2 ст. 284, ч. 3 ст. 284 КПК України). Так, згідно з ч. 3 ст. 284 КПК України провадження щодо юридичної особи підлягає закриттю в разі закриття кримінального провадження щодо вповноваженої особи юридичної особи. Отже, у разі звільнення вповноваженої особи юридичної особи від кримінальної відповідальності на підставі ст. ст. 45–48, ч. 6 ст. 258, ч. 2 ст. 258^3, ч. 4 ст. 258^5 КК України, одночасно виключається і застосування до

юридичної особи примусових заходів кримінально-правового характеру (ст. ст. 96^7, 96^8, 96^9 КК України) [131].

Підводячи підсумки зазначимо, що у підрозділі обставини, що підлягають встановленню під час досудового розслідування шахараств, учинених з використанням ЕОТ, мають значення для правильного вирішення кримінального провадження юридично значимих обставин, які повинні бути доведені або спростовані в цілях обґрунтування висунутого відносно певної особи обвинувачення, а також є фактичною підставою всіх процесуальних рішень, які приймаються. Вказане сприятиме більш якісному і швидкому розслідуванню цих кримінальних правопорушень й посилить обґрунтованість і переконливість позиції державного обвинувача під час судового розгляду кримінальних проваджень даної категорії.

2.2 Типові слідчі ситуації та слідчі версії під час розслідування шахрайств, учинених з використання електронно-обчислювальної техніки

На сучасному етапі розвитку суспільства інформатизація створює інноваційні різновиди злочинних дій, що надають можливість розширенню зони охоплення різних напрямів протиправної діяльності, зокрема шахрайств, що вчиняються з використанням ЕОТ. Недостатня обізнаність слідчих про різновиди типових слідчих ситуацій та відповідних їм слідчих версій призводить до погіршення ефективності початкового етапу розслідування, у зв’язку з невірним визначенням напрямів розслідування, вибору комплексу слідчих дій [211].

Проблематики розслідування кримінальних правопорушень у сфері використання ЕОТ, систем та комп’ютерних мереж і мереж електрозв’язку торкалися в своїх дослідженнях багато вчених, зокрема: Д. С. Азаров, А. І. Анапольська, М. П. Бікмурзін, В. В. Кузнєцов, Ю.Ю. Орлов,

Т. А. Пазинич, О. Е. Радутний, М. В. Рудик, С. В. Самойлов, О. М. Стрільців, С. С. Чернявський, О. М. Юрченко та інші. Проте питання, присвячені дослідженню типових слідчих ситуацій на початковому етапі розслідування шахрайств, учинених з використанням ЕОТ, на сьогодні залишилися недостатньо вивченими.

Першочергово варто зупинитися на короткій характеристиці поняття «Типова слідча ситуація» через призму криміналістичної науки. Термін «слідча ситуація» має значну історію становлення та на сьогодні є одним з найбільш глибоко досліджених як із теоретичного, так і з практичного аспектів.

Серед науковців тривають дискусії щодо цієї категорії. Перший підхід обумовлений тим, до якого розділу криміналістичної науки її варто віднести. Одна група науковців вважає, що вчення про слідчі ситуації тісно пов'язане з дослідженням проблем криміналістичної методики, і розглядають її як конструктивний елемент окремих методик розслідування. Так, М. О. Селіванов вказував, що слідча ситуація здійснює більш значний безпосередній вплив на методику розслідування кримінального правопорушення, ніж криміналістична характеристика. Цей факт потрібно враховувати в процесі планування проведення розслідування [211, с. 58]. Є. С. Хижняк впевнений, що слідча ситуація, як і криміналістична характеристика, є одним із визначальних інструментів слідчого, що надає можливість максимально збільшити ефективність розслідування кримінальних правопорушень, а володіння типовими слідчими ситуаціями дозволяє слідчому виявити коло пріоритетних завдань, мінімізувати вплив чи уникнути нецільової витрати часу та сил. На основі порівняння типової слідчої ситуації та ситуації, що сталася під час розслідування конкретного кримінального правопорушення, використовуючи взаємозв'язки між елементами криміналістичної характеристики цієї групи кримінальних правопорушень, слідчий зможе оптимально спланувати процес розслідування та найефективніше вирішити завдання встановлення особи, яка вчинила

кримінальне правопорушення [244, с. 197].

Інші переконані, що слідча ситуація є категорією криміналістичної тактики. Наприклад, В. К. Весельський вважає, що слідча ситуація належить до кола понять криміналістичної тактики і в цій ролі реалізується в криміналістичній методиці. Це твердження він пояснює тим, що саме слідча ситуація зумовлює тактику конкретних слідчих дій [44, с. 195]. Об'єктивними чинниками, що впливають на слідчу ситуацію, на думку В. К. Весельського, виступають: 1) наявність і характер доказової та орієнтуючої інформації, яка є в розпорядженні слідчого; 2) наявність і стійкість існування ще не використаних джерел доказової інформації та надійних каналів надходження орієнтуючої інформації; 3) інтенсивність процесів зникнення доказів і сила чинників, які впливають на ці процеси; 4) наявність у даний момент у розпорядженні слідчого необхідних сил, засобів, часу і можливість їх оптимального використання; 5) наявна в даний момент кримінально-правова оцінка розслідуваної події. Суб'єктивними чинниками є: 1) психологічний стан осіб, які фігурують у розслідуваній справі; 2) психологічний стан слідчого, рівень його знань і вмінь, практичний досвід, здатність приймати й реалізовувати рішення в екстремальних умовах; 3) протидія встановленню істини з боку злочинця та його зв'язків, а іноді потерпілого та свідків; 4) сприятливий (безконфліктний) перебіг розслідування; 5) зусилля слідчого, спрямовані на зміну слідчої ситуації в бажану сторону; 6) наслідки помилкових дій слідчого, оперативного працівника, експерта; 7) наслідки розголошення даних досудового слідства; 8) непередбачені дії потерпілого або осіб, непричетних до розслідування [44, с. 194–195].

В. В. Кікінчук пропонує під поняттям «типова слідча ситуація» розуміти сукупність умов, даних та інших факторів, які безпосередньо чи опосередковано впливають на особу, яка наділена правовим статусом, у певний момент розслідування нею окремого виду кримінального правопорушення та диктують чітку послідовність інтелектуальної діяльності

як закономірного та властивого кожному розумовому процесу (інколи на підсвідомому рівні), що знаходить своє відображення в прийнятті відповідних процесуально обґрунтованих рішень [100, с. 135].

В. А. Журавель дає таке визначення поняттю «Типова слідча ситуація» – наукова абстракція, яка сформована на підставі апріорних знань, є результатом узагальнення й аналізу значного емпіричного матеріалу і в якій відображено найбільш загальні риси, що характеризують перебіг і стан розслідування на певному етапі (вихідному, початковому, наступному) [78, с. 106].

В. М. Шевчук «типовими слідчими ситуаціями» вважає ті ситуації, з якими стикається слідчий на початковому чи наступному етапі розслідування кримінального правопорушення залежно від повноти вихідних даних. Типові слідчі ситуації суттєво відрізняються від того, за яких умов вчинено кримінальне правопорушення – очевидності чи неочевидності. Виокремлення типових слідчих ситуацій можливе за умови, якщо в основу типізації закладено ставлення підозрюваного до повідомлення про підозру [257, с. 126].

На думку О. Н. Колесниченка та В. О. Коновалової, система першочергових та інших процесуальних дій пов’язана саме з типовими слідчими ситуаціями, чітка побудова яких виконує функції навчання і вирішення завдань практичної діяльності [106, с. 51–52].

Своєю чергою, Р. Л. Степанюк стверджує, що типова слідча ситуація може бути визначена як сформульована на підставі аналізу практики розслідування певної категорії кримінальних правопорушень, абстрагована штучна модель, що відображає стан наявної у слідчого інформації про обставини кримінального правопорушення й обставини, що склалися на певному етапі розслідування [222, с. 111]. С. С. Чернявський вбачає у типовій слідчій ситуації інформаційну модель з найбільш важливими властивостями та ознаками процесу розслідування в кримінальних провадженнях щодо кримінальних правопорушень певної категорії [249, с. 405].

І. В. Калініна розглядає типову слідчу ситуацію як сукупність об’єктивних положень, що виникають передусім на початковому етапі розслідування при незначному обсязі інформації та часто дублюються в практиці розслідування. Інформація про типові слідчі ситуації є результатом узагальнення практики розслідування певного виду кримінальних правопорушень [91, с. 215].

Як зазначає Н. А. Запорощенко, важливе значення має не лише отримання необхідної інформації, але й її оцінка. Серед чинників, що впливають на оцінку слідчим орієнтуючої або доказової інформації, вченою зазначаються такі: 1) сукупність необхідних на певний момент даних, що свідчать про вчинений злочин; 2) наявність необхідної та доступної на даний момент криміналістично значущої інформації; 3) інтенсивність (швидкоплинність) зникнення і знищення слідів кримінального правопорушення та іншої криміналістично значущої інформації про кримінальне правопорушення загалом або його окремі етапи; 4) період часу з моменту вчинення кримінального правопорушення до появи первинної інформації у розпорядженні працівників правоохоронних органів; 5) активність або пасивність суб’єктів доказування і характер їх взаємин; 6) наявність і характер помилок і прорахунків у діях суб’єктів доказування і їх наслідки, що наступили в результаті неправильної реалізації оперативно-розшукового заходу [83, с. 85].

Варто погодитися з думкою Р. С. Степанюка про те, що типізація слідчих ситуацій можлива за умови виділення інформації про окремі найбільш значущі компоненти, що часто зустрічаються, які науковець розподіляє на дві групи. Перша група об’єднує відомості про окремі обставини злочинної діяльності (особу, котра вчинила злочин, сліди кримінального правопорушення, спосіб, предмет посягання та розмір заподіяної злочином шкоди, зв’язки з іншими злочинами). Друга група представлена сукупністю інформації про найбільш важливі обставини розслідування (стан доказової бази, лінію поведінки підозрюваних та інших

учасників розслідування, сторонніх осіб, котрі намагаються втручатися в процес розслідування, можливості слідства тощо) [222, с. 111–112].

Погоджуючись з висловленою думкою, на наш погляд, найбільш цілісний підхід до визначення слідчої ситуації запропонував Г. А. Матусовський, який вказував, що поняття слідчої ситуації можна розглядати у двох аспектах, один з яких охоплює стан самого розслідування на даному етапі та має, так би мовити, внутрішній характер, а інший містить сукупність умов, за яких у даний момент відбувається процес розслідування, і має певний зовнішній характер [145, с. 351].

Зауважимо, що слідчу ситуацію доцільно вважати категорією, яка належить одночасно і до криміналістичної тактики, і до методики. Проте першочергове значення надається криміналістичній методиці, оскільки будь-яка слідча ситуація виникає на початку досудового розслідування, а слідчі дії є лише засобом розслідування. Слідчі ситуації є обов'язковим компонентом процесу розслідування різних кримінальних правопорушень, а типова слідча ситуація – їх окремий вид.

Таким чином, підводячи підсумок, зазначимо, що типові слідчі ситуації мають фундаментальне інформаційне й організаційно-методичне навантаження у визначенні методики розслідування кримінальних правопорушень, а самі типові слідчі ситуації початкового та подальших етапів розслідування є взаємопов'язаними. При цьому типові слідчі ситуації залежать від повноти інформації про: вчинений злочин, зокрема спосіб шахрайства, що учинений з використанням ЕОТ, особистість злочинця, особу потерпілого, предмет посягання та настання злочинних наслідків.

Так, С. В. Самойлов виокремлює три типові слідчі ситуації, які мають місце на початковому етапі розслідування шахрайств, вчинених з використанням мережі «Інтернет»: Ситуація 1. Виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця або встановлено, або достатньо даних для її встановлення. Ситуація 2. Виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет».

Особу злочинця не встановлено, однак є певні відомості, що можуть вказувати на неї. Ситуація 3. Виявлено ознаки шахрайства, що вчиняється з використанням мережі «Інтернет». Особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї [209, с. 26–27].

Беручи до уваги погляди С. В. Самойлова, а також результати узагальнення матеріалів слідчо-судової практики розслідування шахрайств, вчинених з використанням ЕОТ (Додатки Б, В), власний досвід досудового розслідування вказаних кримінальних правопорушень, можна умово виокремити дві основні групи типових слідчих ситуацій на початковому етапі розслідування залежно від характеру первинної інформації про подію та її учасників.

Перша типова слідча ситуація – 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.

Друга типова слідча ситуація – встановлено факт шахрайства з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї.

Зупинимось саме на цих основних двох типових слідчих ситуація, не дивлячись на те, що в практичній діяльності правоохоронних органів НП зустрічаються інші. Наприклад, є в наявності дані про подію вчинення кримінального правопорушення, разом з тим інформація про спосіб вчинення шахрайства невідомий, а установчі дані про особу злочинця, яка його вчинила – відсутні. Або наступний приклад, коли за результатами проведених оперативно-розшукових заходів чи аналізу повідомлень в засобах масової інформації було відкрито кримінальне провадження за фактом вчинення шахрайських дій щодо потерпілого, але останній відмовляється співпрацювати з правоохоронними органами як в частині підтвердження самого такого факту, так і подальшого його розслідування. Разом з тим такі типові слідчі ситуації, зустрічаються в практичній діяльності

вкрай рідко і мають поодинокий характер.

У процесі досудового розслідування шахрайств, учинених з використанням ЕОТ, можуть виникати складні та конфліктні слідчі ситуації [215, с. 366]. Так, складні слідчі ситуації виникають коли відсутні достатньо доказів, тобто не вистачає відомостей про фактичні дані. Також до складних ситуацій можна віднести обставини, коли чиниться протидія слідчим і працівникам оперативних підрозділів. Крім того, у суб'єктів розслідування недостатньо часу, ресурсів і сил. Проблема значно ускладнюється в разі виникнення конфліктної ситуації, яка, по суті, є різновидністю складної слідчої ситуації. За таких обставин стан міжособистісних відносин двох або більше суб'єктів, учасників криміналістичної діяльності є надто напруженим. Адже вони мають інтереси, які не збігаються і прагнуть до досягнення протилежної мети, керуючись індивідуальними планами і намірами [215, с. 91]. Слідчі ситуації можуть виникати і під час проведення конкретних слідчих (розшукових) дій.

Стосовно розуміння сутності версії у криміналістиці серед науковці, як і щодо слідчої ситуації, також немає одностайності, хоча спільні елементи можна знайти у кожному з визначень. Так, Р. С. Бєлкін вважав, що версія є самостійним специфічним криміналістичним засобом, яким користується слідчий для пізнання і доведення об'єктивної істини в попередньому слідстві. Цей засіб полягає у побудові й перевірці слідчим усіх ймовірних на зібраних матеріалах припущень про форми зв'язків і причини окремих явищ події, що розслідується, як реально можливих пояснень, встановлених до теперішнього часу фактів, а також обставин, пов'язаних з даною подією, які можуть знадобитися для перевірки старих і пошуку нових фактів [25, с. 31].

Пояснюючи ґенезу виникнення типових версій, В. О. Коновалова зазначає, що накопичення практики розслідування, її узагальнення й аналіз дозволили виявити певні залежності при вчиненні окремих видів кримінальних правопорушень, котрі існують як свого роду стандарти, що мають місце в практиці розслідування. Такого роду залежності притаманні

всім видам учинених кримінальних правопорушень і зазвичай розглядаються як типові, що найбільш часто зустрічаються, версії, які виникають у процесі розслідування, але, будучи предметом узагальнення, виступають як незалежні типові припущення, наявні в теоретичних рекомендаціях криміналістичної методики [110, с. 60–61].

О. М. Цільмак вбачає у криміналістичній версії об'єктивне припущення або висновок стосовно певного кримінального правопорушення, що виникає з фактичних підстав і логічних міркувань, вимагає відповідної перевірки, спрямоване на з'ясування істини у кримінальному провадженні. Автор наводить досить розширену їх класифікацію, а саме: 1) за часом виникнення: первинні (початкові), які виникають відразу; вторинні (наступні), які виникають у процесі вивчення фактичних даних та інформації; 2) за значенням для правозастосовної діяльності: провідні, які є головними, основними; допоміжні, які уточнюють і доповнюють провідні версії; запасні, які не заперечуються, однак є менш ймовірними; відкинуті, які не мають значення для правозастосовної діяльності; 3) за терміном необхідності їх перевірки: першочергові, тобто, які необхідно перевірити у першу чергу; другорядні, тобто, які мають другорядне значення для перевірки; 4) за обсягом: односкладні, тобто, які висунуті за однією обставиною; багатоскладні, тобто, які висунуті стосовно кількох обставин; 5) за об'ємом: загальні, які визначають оцінку розслідуваної події загалом; приватні, які стосуються окремих обставин загальної версії; 6) за суб'єктом висунення: слідчі; оперативно-розшукові, експертні, судові, версії обвинувачення (прокурора), версії захисту (захисника); 7) за ступенем конкретності: узагальнені (типові), тобто, які пояснюють подію загалом на підставі даних науки та узагальненого досвіду практики; конкретні, тобто, робочі версії, над якими працює у той або інший момент суб'єкт правозастосовної діяльності; 8) за ступенем ймовірності: найбільш ймовірні, мало ймовірні, неймовірні; 9) за характером відношення до предмета доказування: обвинувальні та виправдувальні; 10) за спрямованістю у часі: ретроспективні, тобто їх

предметом є події минулого, сам факт вчинення кримінального правопорушення та окремі його обставини; перспективні, тобто ті, які спрямовані на прогнозування та передбачення того, що може статися; 11) за способом вирішення проблемних ситуацій: пошукові, тобто, які спрямовані на пошук джерел (носіїв) інформації; дослідницькі, тобто, які спрямовані на дослідження вже виявленої інформації; 12) за формою конструювання: логічні, тобто, які виходять з фактичних даних і наявної інформації; інтуїтивні, тобто, які є несвідомими, суб'єкт висунення не може їх логічно обґрунтувати, але вони теж засновані на якихось знаннях, розумінні психології людини тощо [246, с. 334–335].

Роль версій у пізнанні розслідуваної події надзвичайно велика. Системи типових версій визначають головні напрями діяльності слідчого, специфіку завдань, що підлягають розв'язанню. При цьому, чим більш повно буде представлена ця система, тим більша ймовірність збігу типового з конкретним, а відтак і більша можливість побудови найпродуктивнішої робочої слідчої версії на підставі типових, що входять до запропонованої системи [213, с. 88]. Також слідчі версії складають логічну основу плану розслідування кримінального правопорушення. Найбільш раціональним є план, складений за кожною висунутою версією, з виокремленням у його загальну частину питань, що підлягають з'ясуванню за всіма версіями [123, с. 157].

У зв'язку з цим, вказує В. В. Семеногов, наявні дві проблеми, розв'язання яких визначає ефективність розслідування, досягнення об'єктивної істини. Перша проблема – пізнавальна роль версії, її функція як методу пізнання в конкретній галузі, якою є судочинство. Друга проблема – методи побудови версій у різних ситуаціях розслідування: а) при обмеженні доказової інформації; б) при її відсутності взагалі; в) при її значному обсязі. Побудова слідчих версій визначається видом вчиненого кримінального правопорушення, способом його вчинення та приховування, тобто спирається на початкову слідчу ситуацію [212, с. 80].

Таким чином, криміналістична версія – це обґрунтоване припущення особи, уповноваженої здійснювати діяльність з виявлення та розслідування кримінальних правопорушень щодо фактів, явищ або групи фактів чи явищ, які мають або можуть мати значення для кримінального провадження й свідчать про сутність події, що досліджується; про причини, які їх зумовили; про винних осіб, характер їхньої вини та інші обставини, що сприяють встановленню істини у кримінальному провадженні [59, с. 35].

Узагальнення матеріалів практики та власний досвід дозволяє визначити, що під час розслідування шахрайств, учинених з використанням ЕОТ, можна висунути наступні типові слідчі версії:

– *щодо наявної інформації про особу злочинця:*

1) шахрайство з використанням ЕОТ вчинене відомою для потерпілого особою або особою, щодо якої є достатньо даних для її встановлення;

2) шахрайство з використанням ЕОТ вчинене невідомою для потерпілого особою;

– *щодо механізму вчинення шахрайства та побудови вебсторінки, яку використовували для вчинення кримінального правопорушення:*

1) шахрайство вчинене особою, які має поверхневі знання у користуванні ЕОТ;

2) шахрайство вчинене особою, яка є спеціалістом у сфері інформаційних технологій;

– *щодо кількості злочинців:*

1) шахрайство з використанням ЕОТ вчинене одноособово;

2) шахрайство з використанням ЕОТ вчинене групою осіб;

3) шахрайство з використанням ЕОТ вчинене організованою злочинною групою;

– *щодо обізнаності осіб про співучасників шахрайства:*

1) особа (виявлений злочинець) має інформацію про інших співучасників (членів групи) і може назвати їх;

2) особа (виявлений злочинець) не має інформації про інших співучасників групи, так як останні були одноразово залучені для виконання певної ролі під час вчинення кримінального правопорушення, між собою не знайомі та не є постійними членами злочинної групи;

3) особи, що сприяли у вчиненні кримінального правопорушення, не були поінформовані про злочинні дії злочинця, не мали наміру заволодіти майном чи правом на майно, а лише виконували дії, які вказував їм злочинець та які не заборонені законодавством України (наприклад, розробка сайту, надання послуг з його розміщення, розробка програмних засобів тощо) [209, с. 28–29];

– *щодо кількості вчинених кримінальних правопорушень:*

1) шахрайство з використанням ЕОТ вчинене вперше;

2) шахрайство з використанням ЕОТ вчинене неодноразово;

– *щодо поширеності шахрайства:*

1) обмежена кількість шахрайств;

2) регіональне поширення шахрайського посягання;

3) шахрайства вчиняються на державному рівні;

4) шахрайства вчиняються на міждержавному рівні;

– *щодо місця розташування ЕОТ, з якого злочинці вчиняли контакти з потерпілим:*

1) особи, які причетні до вчинення шахрайства, використовували ЕОТ, яка розташована на території України;

2) особи, які причетні до вчинення шахрайства, використовували ЕОТ, яка розташована за межами території України;

3) особи, які причетні до вчинення шахрайства, використовували ЕОТ, яка розташована на тимчасово окупованій території у Донецькій та Луганській областях або анексованій Автономній Республіки Крим;

– *щодо кількості потерпілих:*

1) шкоду завдано лише потерпілим, які звернулися з відповідною заявою;

2) потерпілих від злочинної діяльності значно більше, але вони не звернулися до правоохоронних органів з різних причин (через сором, що їх ошукали; через незнання, що вчинені зловмисником дії є кримінальним правопорушенням; через відсутність довіри до правоохоронних органів тощо) [29, с. 28].

Також слідчі версії можуть висуватися за результатами аналізу IP-адрес, за якими здійснювалось використанням ЕОТ з метою вчинення шахрайства: 1) для вчинення шахрайства використовувалась одна IP-адреса; 2) для вчинення шахрайства використовувалось декілька IP-адрес; 3) для вчинення шахрайства використовувались невстановлені IP-адреси.

Під час розслідування шахрайств, учинених з використанням ЕОТ, особливий інтерес викликають контрверсії (версії захисту), оскільки вони є найменш дослідженими. Якщо слідчий не візьме до уваги можливе висунення контрверсій, вони створюють певні труднощі під час розслідування такого виду шахрайства, що обумовлює необхідність їх перевірки з метою всебічності та об'єктивності розслідування. Практичний досвід розслідування шахрайств, учинених з використанням ЕОТ, засвідчив що контрверсії можуть висуватися з приводу будь-яких обставин події кримінального правопорушення, зокрема:

– підозрюваний заявляє, що ЕОТ, яка фігурує як засіб вчинення шахрайства, не належить йому, а її користувачем є інша особа, яка йому лише уявно відома. Підозрюваний просто надавав ЕОТ іншій особі в оренду чи просто безоплатно для користування;

– електронно-обчислювальну техніку, яка фігурує як засіб вчинення шахрайства, підозрюваний придбав вже після вчинення кримінального правопорушення;

– підозрюваний не знав, що він вчиняє шахрайство, так як предмет посягання він хотів передати у майбутньому через деякий час. І цю обставину підозрюваний пов'язує з проблемою відправки предмету посягання чи відсутністю своєчасної поставки цього предмета з іншої країни;

– підозрюваний відводить собі другорядну роль під час вчинення шахрайства з використанням ЕОТ;

– виявлені при обшуках записи підозрюваний пояснює тим, що він самостійно вирішив підвищувати свій інтелектуальний рівень з метою більш поглибленого вивчення якого-небудь предмета (зазвичай таких, які вивчають у вищих навчальних закладах).

У зв'язку з наявністю таких контрверсій слідчий включати їх до плану розслідування, своєчасно проводити слідчі (розшукові) чи негласні слідчі (розшукові) дії щодо їх перевірки.

Підводячи підсумки до підрозділу зазначимо, що під час розслідування шахрайств, учинених з використанням ЕОТ, можуть виникати типові слідчі ситуації, аналіз яких допомагає обрати напрям розслідування кримінального правопорушення та оптимізувати процес дій слідчого, а також вимагає висунення та перевірки слідчих версій.

З урахуванням вихідної інформації слідчі версії можуть висуватися щодо: особи злочинця; механізму вчинення шахрайства та побудови вебсторінки, яку використовували для вчинення кримінального правопорушення; кількості злочинців; співучасників шахрайства; кількості вчинених кримінальних правопорушень; поширеності шахрайства; місця розташування ЕОТ з якого злочинці вчиняли контакти з потерпілим; мотиву вчинення шахрайства; виду носія слідів, які виявлені у зв'язку з використанням ЕОТ з метою вчинення шахрайства. Під час розслідування шахрайств, учинених з використанням ЕОТ, можуть виникати контрверсії (версії захисту) з приводу будь-яких обставин події кримінального правопорушення.

У розвиток кожної з вказаних вище версій надалі висуваються окремі версії, що базуються на конкретних даних, зібраних у кримінальному провадженні, найбільшої уваги серед яких заслуговують окремі версії, що стосуються особи, яка вчинила кримінальне правопорушення.

2.3 Основні напрями розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки

Проблемам розслідування шахрайств, які вчиняються з використанням ЕОТ, у різний час приділялася увага у роботах Д. С. Азарова, А. І. Анапольського, Б. В. Андрєєва, Р. С. Атаманова, О. А. Баранова, Ю. М. Батуріна, В. М. Бутузова, Т. В. Варфоломеєва, М. С. Вертузаєва, О. Г. Волєводза, В. Д. Гавловського, С. В. Головкіна, В. О. Голубєва, В. Г. Гончаренка, В. А. Губанова, М. В. Гуцалюка, Д. О. Зикової, М. І. Камлика, М. В. Карчевського, Н. Ю. Кириленка, С. М. Князєва, В. А. Колесника, А. А. Комарова, О. І. Котляревського, А. В. Крижевського, В. В. Крилова, О. В. Курмана, В. Д. Ларичева, А. К. Лебедєва, О. В. Лисодєда, В. Б. Міщенка, О. І. Мотляха, О. Л. Мусієнка, В. І. Оборського, Т. В. Охрімчука, Т. А. Пазинича, Л. П. Паламарчука, Б. В. Романюка, С. В. Самойлова, О. В. Смаглюка, О. М. Стрільціва, О. І. Усова, В. П. Хорста, В. С. Цимбалюка, С. С. Чернявського, В. П. Шеломенцева, О. М. Юрченка та інших.

Потрібно відзначити, що проведені дослідження стосувалися різних груп шахрайства (у сфері обігу житла, цінних паперів, страхування) і не враховували особливостей розслідування окремого різновиду шахрайств, учинених з використанням ЕОТ.

Як зазначалося у попередньому підрозділі, за результатами узагальнення матеріалів слідчо-судової практики розслідування шахрайств, вчинених з використанням ЕОТ, було сформульовано дві основні групи типових слідчих ситуацій на початковому етапі розслідування залежно від характеру первинної інформації про подію та її учасників.

Перша типова слідча ситуація – 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, визначено чи є достатньо даних для її встановлення.

Друга типова слідча ситуація – встановлено факт шахрайства з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї.

З поняттям етапу розслідування у криміналістичній методиці тісно пов'язане поняття слідчої ситуації, яке відіграє важливу роль у формуванні практичних рекомендацій з розслідування кримінальних правопорушень. Розслідування шахрайства здійснюється в конкретних умовах, пов'язаних з часовими межами, місцем учинення, способами вчинення шахрайства, взаємозалежністю з іншими процесами об'єктивної дійсності, поведінкою учасників кримінального судочинства. Ця складна система взаємозв'язків у кінцевому підсумку формує обстановку, у якій доводиться діяти слідчому [97, с. 97].

Щодо першої слідчої ситуації основні сили слідчого повинні бути спрямовані на встановлення місцезнаходження ЕОТ, правильне закріплення слідів причетності ЕОТ та осіб, які могли нею користуватися, до кримінального правопорушення (слідів роботи комп'ютерної системи, електронної чи телефонної переписки злочинця з потерпілим), а також перевірку причетності до протиправних діянь інших осіб.

З цією метою проводяться наступні процесуальні дії:

1. Отримання та реєстрація в Єдиному реєстрі досудових розслідувань (ст. 214 КПК України) заяви, повідомлення про вчинення кримінального правопорушення, пов'язаного з шахрайством.

2. Підготовка та виїзд слідчо-оперативної групи на місце події.

3. Здійснення огляду місця події у потерпілої особи. Як правило, огляд місця події представляє собою службове або житлове приміщення, де розташована ЕОТ, з яких потерпіла особа здійснювала вихід в мережу Інтернет за допомогою засобів комп'ютерної техніки, переглядала сайти чи соціальні мережі, здійснювала листування зі злочинцем, робила замовлення товарів чи послуг, переказувала кошти, які були предметом шахрайства тощо. Огляду підлягають безпосередньо ЕОТ з метою визначення установчих

даних власників вебсайту чи інтернет-ресурсу або власника сторінки в соціальній мережі, які використовувалися у протиправних цілях, і дозволяють ідентифікувати особу, яка вчинила шахрайство; з'ясування електронної скриньки потерпілого, на яку надсилались листи від злочинця.

4. Внесення до Єдиного реєстру досудових розслідувань відомостей, отриманих за результатами огляду місця події, відкриття кримінального провадження, початок досудового розслідування та направлення письмового повідомлення про це прокурору (ч. 6 ст. 214 КПК України).

5. Допит потерпілого, під час якого з'ясовуються всі обставини вчинення шахрайства з використанням ЕОТ, встановлення особи, яка може бути причетна до цього кримінального правопорушення і про яку потерпілий володіє інформацією. Одержані докази можуть бути успішно використані на допиті підозрюваного для доведення його причетності до вчиненого кримінального правопорушення.

6. Допит свідків (за наявності таких), яким відомі обставини шахрайства, учиненого з використанням ЕОТ, а також які знають підозрюваного або мають інформацію про факти вчинення ним протиправних діянь. В якості свідків часто виступають працівники оперативних підрозділів, які здійснюють оперативний супровід досудового розслідування та яким під час ОРД стають відомі певні факти щодо конкретного способу, дати, часу, місця та особи шахрая.

7. Надання письмових доручень оперативним підрозділам Національної поліції з метою встановлення IP-адрес інтернет-ресурсу (вебсайту), ЕОТ і засобів комунікації, які використовувались з метою вчинення шахрайства.

8. За ухвалою слідчого судді проведення обшуку приміщень за місцем встановлення ЕОТ ізасобів комунікації, які були визначені інтернет-провайдерами. У разі необхідності проведення обшуку за місцем проживання або роботи осіб, які можуть бути причетні до вчинення шахрайських дій з використанням ЕОТ.

9. Призначення судових експертиз і направлення на експертизу вилучених під час обшуку речей та документів.

Якщо особу, яка може бути причетна до вчинення шахрайства з використанням ЕОТ, встановлено, типовими є наступні процесуальні дії та заходи:

1. Повідомлення особі про підозру та її допит як підозрюваного у вчиненні шахрайства з використанням ЕОТ.

2. Обрання запобіжного заходу та вжиття інших заходів забезпечення кримінального провадження.

3. Зібрання даних, що характеризують особу підозрюваного.

4. Перевірка підозрюваного за всіма обліками на предмет визначення його судимості, можливих кримінальних зв'язків за минулими судимостями і т. ін.

5. Проведення (за необхідності) пред'явлення підозрюваного для впізнання потерпілим (свідкам) з подальшим проведенням між ними у разі потреби одночасних допитів. Вказана процесуальна дія може здійснюватись з метою пред'явлення для впізнання за голосом підозрюваного, у випадках коли потерпілий його не бачив.

6. За ухвалою слідчого судді проведення обшуку за місцем проживання та роботи підозрюваного (якщо такі не були проведені раніше) з метою виявлення доказів причетності до вчинення шахрайства, отримання порівняльних зразків.

7. Призначення за необхідності судово-психіатричної експертизи підозрюваного.

8. За ухвалою слідчого судді відібрання (отримання) зразків у підозрюваного, необхідних для проведення експертизи, наприклад, зразків волосся, дактелоскопіювання тощо та призначення експертиз щодо вилучених предметів.

9. За ухвалою слідчого судді здійснення тимчасового доступу до документів інтернет-провайдерів з метою отримання інформації щодо

користувачів інтернет-сайтів і власників поштових скриньок підозрюваного: а) про реєстрацію доменного імені та хостінгу, з якого здійснювались шахрайські дії; б) про реєстрацію IP-адреси чи поштової скриньки інтернет-мережі; в) про адміністрування інтернет-форуму або чату, через який підозрюваний здійснював спілкування з потерпілим під час вчинення шахрайських дій щодо нього.

10. За ухвалою слідчого судді здійснення тимчасового доступу до речей та документів, які могли використовуватись з метою вчинення шахрайства, або на них зафіксовано сліди вчинення шахрайства з використанням ЕОТ, а саме: до банківських установ про рахунки, які належать потерпілому або іншим юридичним та фізичним особам, які використовувались під час вчинення шахрайських дій, а також про рух коштів по таких рахунках; до інтернет-провайдера – щодо надання інформації про IP-адреси підозрюваного, його електронну скриньку; операторів телефонного зв'язку – щодо доступу до переписки та дзвінків підозрюваного; до камер спостереження та огляд записів, у яких зафіксовано перебування підозрюваного у приміщеннях чи інших місцях, де він виходив у мережу Інтернет.

11. Слідчий огляд вилученого під час обшуку та тимчасового доступу до речей і документів (ЕОТ, відеозаписи, грошові кошти, документи на переказ, чорнові записи, банківські платіжні картки тощо).

12. Тимчасовий доступ до банківських установ з метою отримання інформації про рахунки, які належать юридичним і фізичним особам, які використовувались під час вчинення шахрайських дій, а також про рух коштів по таких рахунках, а також надання інформації про банківські перекази від потерпілого до підозрюваного.

13. Тимчасовий доступ до операторів телефонного зв'язку – щодо доступу до переписки та дзвінків підозрюваного, який спілкувався з потерпілим під час вчинення шахрайства.

14. За потреби проведення негласних (слідчих) розшукових дій – обстеження публічно недоступних місць, житла та іншого володіння особи, аудіо- та відеоконтроль особи [78; 206, с. 123–124; 223, с. 21–24].

Що стосується слідчої ситуації, коли особа, яка вчинила шахрайство з використанням ЕОТ, невідома, основними напрямами дій слідчого є встановлення місцезнаходження ЕОТ та визначення кола осіб, які можуть бути причетні до вчинення такого виду шахрайства. З цією метою здійснюються наступні процесуальні дії, які частково співпадають з попередніми, але мають свої відмінності:

1. Отримання та реєстрація в Єдиному реєстрі досудових розслідувань (ст. 214 КПК України) заяви, повідомлення про вчинення кримінального правопорушення, пов’язаного з шахрайством.

2. Підготовка та виїзд слідчо-оперативної групи на місце події.

3. Проведення огляду місця події у потерпілої особи. Як правило, огляд місця події представляє собою службове або житлове приміщення, де розташована ЕОТ, з яких потерпіла особа здійснювала вихід в Інтернет мережу за допомогою засобів комп’ютерної техніки, переглядала сайти чи соціальні мережі, здійснювала листування зі злочинцем, робила замовлення товарів чи послуг, переказувала кошти, які були предметом шахрайства тощо. Огляду підлягають безпосередньо ЕОТ з метою визначення установчих даних власників вебсайту чи інтернет-ресурсу або власника сторінки в соціальній мережі, які використовувалися у протиправних цілях і дозволяють ідентифікувати особу, яка вчинила шахрайство; з’ясування електронної скриньки потерпілого, на яку надсилались листи від злочинця.

4. Внесення до Єдиного реєстру досудових розслідувань відомостей, отриманих за результатами огляду місця події, відкриття кримінального провадження, початок досудового розслідування та направлення письмового повідомлення про це прокурору (ч. 6 ст. 214 КПК України) [131].

5. Допит потерпілого, під час якого з'ясовуються всі обставини вчинення шахрайства з використанням ЕОТ. Якщо потерпілий не володіє відомостями про осіб, які причетні до шахрайства, слідчий повинен акцентувати увагу на деталізації спілкування потерпілого зі злочинцем, способі вчинення шахрайства.

10. Допит свідків (за наявності таких), яким відомі обставини вчиненого кримінального правопорушення, пов'язаного з шахрайством, учиненого з використанням ЕОТ. Часто допитують працівників оперативних підрозділів, які здійснюють оперативний супровід досудового розслідування та яким під час ОРД стають відомі певні факти щодо конкретного способу, дати, часу, місця та особи шахрая.

6. У разі необхідності призначення судових експертиз і направлення на експертизу вилученої за результатами огляду місця події інформації завдяки якій можливо встановити IP-адреси ЕОТ злочинця, інтернет-ресурсу, який використовувався у протиправних цілях, способи спілкування злочинця з потерпілим.

7. Надання письмових доручень оперативним підрозділам Національної поліції з метою встановлення IP-адрес інтернет-ресурсу (вебсайту), ЕОТ і засобів комунікації, які використовувались з метою вчинення шахрайства.

8. Надання письмових доручень оперативним підрозділам на проведення негласних (слідчих) розшукових дій, спрямованих на встановлення IP-адрес Інтернет-ресурсу (вебсайту), ЕОТ і засобів комунікації, які використовувались з метою вчинення шахрайства.

9. За результатами отриманої від оперативних підрозділів інформації здійснюється тимчасовий доступ до документів інтернет-провайдерів з метою отримання інформації щодо осіб, причетних до створення (власників) інтернет-ресурсу (вебсайту), осіб, які здійснюють їх адміністрування, а також безпосередніх користувачів: а) про реєстрацію доменного імені та хостінгу, з якого здійснювалось шахрайство; б) про реєстрацію IP-адреси чи поштової

скриньки користувача Інтернет-мережі, причетного до шахрайства, учиненого з використанням ЕОТ; в) про адміністрування інтернет-форуму або чату, через який здійснювалося спілкування потерпілого під час вчинення шахрайських дій щодо нього.

10. За результатами отриманої від оперативних підрозділів інформації за ухвалою слідчого судді здійснюється зняття інформації з електронних інформаційних систем щодо поштових скриньок, які використовувались для спілкування з метою вчинення шахрайства.

11. За ухвалою слідчого судді здійснюється тимчасовий доступ до речей та документів, які могли використовуватись з метою вчинення шахрайства, або на них зафіксовано сліди вчинення такого кримінального правопорушення. Такий тимчасовий доступ здійснюється, насамперед, до провайдерів програмних послуг та інтернет-провайдерів з метою встановлення: коли та протягом якого часу було створено певний обліковий запис за певною IP-адресою; якими є реквізити абонента, який здійснював доступ до мережі Інтернет під певною IP-адресою у певний час доби; з якої IP-адреси було створено обліковий запис користувача, який створив Інтернет-ресурс; які IP-адреси використовувалися для створення певного облікового запису; на кого зареєстрований обліковий запис (повні анкетні дані власників сайту, інформація з панелі адміністрування, IP-адреси, номери телефонів тощо); які IP-адреси використовуються для з'єднання з цим обліковим записом; деталізація всіх IP-адрес і часу виходу у даний обліковий запис користувача; якими є реєстраційні дані (logs) та абонентська інформація про користувача певного облікового запису (електронної поштової адреси); як здійснювався перегляд даного облікового запису та його наповнення (IP-адреса, установчі дані та час входу); яким чином оплачуються послуги за зазначене доменне ім'я (вид платіжної системи, яка використовувалась при поповненні балансу облікового запису користувача даної системи (гаманці, ідентифікатори, види оплат), банківські установи, рахунки тощо; яким є зміст адресної книги електронної поштової скриньки;

якими є зміст усіх вхідних і вихідних повідомлень; установчі дані користувача поштової скриньки; через який телефонний номер здійснювалась активація облікового запису; якими є деталі всіх сеансів входу до даного облікового запису із зазначенням IP-адрес та часу [224, с. 31–32]. Для спрямування запитів з метою встановлення закордонних інтернет-користувачів варто використовувати можливості Робочого апарату Укрбюро Інтерполу Національної поліції України для зв'язку з правоохоронними органами тієї держави, де розташовано головний офіс інтернет-провайдера.

12. За ухвалою слідчого судді здійснюється тимчасовий доступ до операторів телефонного зв'язку – щодо доступу до переписки та дзвінків особи, яка спілкувалась з потерпілим під час вчинення шахрайства.

13. За ухвалою слідчого судді здійснюється установлення місцезнаходження радіоелектронного засобу, а саме мобільного телефону, який належить злочинцю, з метою локалізації місцезнаходження такого телефону.

14. За ухвалою слідчого судді здійснюється тимчасовий доступ до інформації, яка була відзнята камерами відеоспостереження чи відеореєстраторами за місцем вчинення кримінального правопорушення та проведення подальшого огляду таких записів з метою встановлення осіб у приміщеннях чи інших місцях, з яких виходив у мережу Інтернет з використанням ЕОТ за певною IP-адресою.

15. Надання доручення оперативному підрозділу НП України в порядку ст. 40 КПК України на проведення комплексу інших негласних слідчих (розшукових) дій, спрямованих на встановлення місцезнаходження ЕОТ, яка використовувалась під час шахрайства, проведення організаційних заходів з метою персоналізації відомостей про користувачів, а також пошуку інформації в інформаційно-пошукових системах Національної поліції.

16. Приєднання до кримінального провадження документів і протоколів з відповідними додатками, які отримані в результаті проведення НСРД відповідно КПК України [132] та Інструкції про організацію

проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджену наказом Генеральної прокуратури України, МВС України, Служби безпеки України, Адміністрації державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5 [90].

17. За ухвалою слідчого судді проводяться обшуки у приміщеннях за місцем встановлення ЕОТ і засобів комунікації, IP-адреси яких використовувались для вчинення шахрайських дій з використанням ЕОТ.

18. Призначення судових експертиз і направлення на експертизу вилучених під час обшуку та тимчасового доступу речей і документів [78; 196; 206, с. 123–124; 223, с. 21–24].

Важливим напрямом встановлення осіб, які вчиняють шахрайство з використанням ЕОТ, є здійснення процесуальних дій щодо коштів або майна, які були предметом такого кримінального правопорушення. З цією метою здійснюються наступні дії:

1. Отримання у потерпілого платіжних документів, які підтверджують факт внесення ним грошових коштів на банківський рахунок.

2. За ухвалою слідчого судді здійснюється тимчасовий доступ до банківських установ про рахунки, які належать юридичним та фізичним особам, і при цьому використовувались під час вчинення шахрайських дій, а також про рух коштів по таких рахунках й надання інформації про банківські перекази від потерпілого до злочинця.

3. Здійснення аналізу отриманих матеріалів від банків і банківських установ (банківських рахунків), а саме дослідження інтернет-трафіку, який використовувався під час користуванням банківськими рахунками, на які були переведені кошти потерпілим. Зазвичай, з метою приховування своєї протиправної діяльності, пов’язаної з шахрайством, учиненим з використанням ЕОТ, злочинці створюють та адмініструють (перевіряють) рахунки з використанням Інтернет-мережі, при цьому в саму систему вони

заходять за допомогою програм VPN або їх аналогів з метою приховування IP-адрес і забезпечення конфіденційного зв'язку. Разом з тим, в окремих випадках, злочинці можуть за необережністю увійти в банківську систему через відкритий трафік (не через VPN), і таким чином засвітити IP-адреси, які зареєстровані в нашій державі.

4. Надання письмових доручень оперативним підрозділам на проведення негласних (слідчих) розшукових дій, спрямованих на встановлення IP-адрес, які використовувались особами для входу в банківську систему.

5. За ухвалою слідчого судді здійснюється тимчасовий доступ або обшук (залежно від обставин) у приміщенні, де зареєстровані IP-адреси, які використовувались для входу у банківську систему.

6. Проведення огляду камер відеоспостереження в приміщенні банку, де знімались грошові кошти, які були спрямовані (перераховані) потерпілим.

7. Надання доручення оперативним підрозділам встановити особу, яка отримала грошові кошти, перевірити її на причетність до вчинення шахрайства [165, 196].

Якщо особа не була встановлена за результатами попередніх процесуальних дій, то в даному випадку подальшими напрямами діяльності слідчого є проведення інших процесуальних дій, насамперед, негласних слідчих (розшукових) дій, спрямованих на встановлення місцезнаходження ЕОТ, яка використовувалась під час вчинення шахрайства, а також встановлення осіб, які можуть бути причетні до цього кримінального правопорушення.

Якщо особу встановлено, здійснюються наступні процесуальні дії та заходи:

1. За ухвалою слідчого судді проводиться обшук за місце проживання чи роботи підозрюваного, а також у місць, з яких підозрюваний здійснював створення, адміністрування інтернет-ресурсу (вебсайту, чату)

(якщо такі не були проведені раніше) з метою виявлення доказів злочинної діяльності щодо причетності певних осіб до вчинення шахрайства.

2. Повідомлення особі про підозру та її допит як підозрюваного у вчиненні шахрайства з використанням ЕОТ.

3. Обрання запобіжного заходу та вжиття інших заходів забезпечення кримінального провадження.

4. Зібрання даних, що характеризують особу підозрюваного.

5. Перевірка підозрюваного за всіма обліками на предмет визначення його судимості, можливих зв'язків за минулими судимостями і т. ін.

6. Проведення (за необхідності) пред'явлення підозрюваного для впізнання потерпілим (свідкам) з подальшим проведенням між ними у разі потреби одночасних допитів. Вказана процесуальна дія може здійснюватись з метою пред'явлення для впізнання за голосом підозрюваного, у випадках коли потерпілий його не бачив.

7. Призначення за необхідності судово-психіатричної експертизи підозрюваного.

8. За ухвалою слідчого судді відібрання (отримання) зразків у підозрюваного, необхідних для проведення експертизи, наприклад, зразків волосся, дактилоскопіювання тощо та призначення експертиз щодо вилучених предметів.

9. Слідчий огляд вилученого під час обшуку та тимчасового доступу речей і документів (ЕОТ, відеозаписи, грошові кошти, документи на переказ, чорнові записи, банківські платіжні картки тощо) [78; 206, с. 123–124; 223, с. 21–24].

Перелік процесуальних дій, які найчастіше проводяться під час досудового розслідування даної категорії кримінальних проваджень, засвідчило проведене опитування слідчих: затримання підозрюваного та його допит (зазначили 100,0 %), обшук місця знаходження ЕОТ, з використанням якої здійснювалось шахрайство (99,3 %), призначення експертиз (92,7 %),

обшук житла чи іншого володіння підозрюваного (63,9 %), пред'явлення речей для впізнання (51,0 %), негласні слідчі (розшукові) дії (49,3 %), тимчасовий доступ до речей і документів (50,3 %), особистий обшук затриманої особи (40,3 %), наведення довідок (37,0 %), огляд місця події – робоче місце потерпілого (35,3 %), допит свідків (18,6 %), одночасний допит двох і більше вже допитаних осіб (12,3 %), пред'явлення особи для впізнання (11,0 %), освідування особи (зазначили 2,3 %), слідчий експеримент (1,3 %), отримання зразків для експертизи (0,6 %) (Додаток Б).

Вина осіб, причетних до шахрайства з використанням ЕОТ, може бути також доведена:

– результатами дослідження способів спілкування (обміну інформацією) потерпілого з підозрюваним через мережу Інтернет, а саме їх переписка через електронну пошту або в чаті;

– юридичним зв'язком підозрюваного з роботою на певній ЕОТ, через яку здійснювалось розміщення підозрюваним даних про об'єкт шахрайства в Інтернет-мережі, подальша модерація (адміністрування) такого повідомлення (наявність облікових записів електронної пошти, наявність кешу у браузері ЕОТ, залишення в пам'яті ЕОТ слідів активності в Інтернет-мережі та безпосередньо в ЕОТ тощо);

– результатами дослідження змісту жорсткого диску ЕОТ підозрюваного зі слідами журналів роботи в Інтернет-мережі (закладки, пошукові запити), тимчасових файлів (кеш, Cookie-файли, буфер друку, місце зберігання інформації, записаної на комп'ютер вебсайтом), змісту своп-файла «вільне місце», списків друзів + особистих профілів + записів чат-кімнат + інших збережень «області»; відстеженням дат збереження файлів (у файлі Windows зберігаються дати створення (коли файл був створений), останнього запису (коли файл востаннє був змінений) та останнього доступу до файлу (коли файл востаннє був відкритий) [224, с. 22];

– результатами дослідження користування банківськими рахунками на які були переведені кошти від потерпілої особи внаслідок вчинення щодо неї

шахрайства з використанням ЕОТ;

– іншими документами, які засвідчують про протиправну діяльність особи – інформація про створення адміністрування банківського рахунку підозрюваного з певної ЕОТ, наприклад, зняття коштів, після перерахування їх потерпілими на ці рахунки, або подальше перерахування коштів третім особам, з якими підозрюваний підтримує зв'язок.

Важливим компонентом досудового розслідування шахрайств, учинених з використанням ЕОТ, є проведення НСРД, передусім, з метою встановлення місцезнаходження ЕОТ, встановлення причетності осіб, які використовували ЕОТ з метою вчинення шахрайства, а також розшуку осіб, які причетні до вчинення цього кримінального правопорушення. Відмітимо найбільш ефективні НСРД, які необхідно проводити з вказаною вище метою:

– зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України) (мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу), яке проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження [239, с. 112–113];

– зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України) [132] полягає в одержанні інформації, зокрема із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютерах), автоматичних системах, комп'ютерній мережі [239, с. 112–113];

– установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) [132] полягає в застосуванні технічних засобів (технічного обладнання) для локалізації місцезнаходження радіоелектронного засобу, зокрема мобільного терміналу систем зв'язку, та інших радіовипромінювальних пристроїв, активованих у мережах операторів

рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються [239, с. 114–115];

– спостереження за особою в публічно доступних місцях (ст. 269 КПК України) [132] полягає у візуальному спостереженні за особою слідчим чи уповноваженою особою для фіксації *з* використанням відеозапису, фотографування її пересування, контактів, поведінки, перебування в певному публічно доступному місці тощо або застосуванні з цією метою спеціальних технічних засобів для спостереження [239, с. 115–116].

Підводячи підсумки, зазначимо, що визначеним у дисертації типовим слідчим ситуаціям притаманні певні алгоритми дій, що обумовлено сукупністю конкретних обставин. Для кожної слідчої ситуації притаманні характерні процесуальні дії, виконання яких здійснюється у певній послідовності, які можна узагальнити за наступними напрямами: а) встановлення місцезнаходження ЕОТ, яка використовувалася з метою вчинення шахрайства; б) встановлення особи, яка причетна до використання ЕОТ з метою вчинення шахрайства; в) встановлення осіб, які отримали кошти, майно, право на майно чи інформацію за результатами вчинення шахрайства, використовуючи ЕОТ.

Таким чином, комплекс процесуальних дій при розслідуванні шахрайства перебуває у прямій залежності від характеру слідчої ситуації, і зміна останньої веде до перегляду системи розслідування кримінального правопорушення. При цьому, вважаємо можливим використовувати для типізації слідчих ситуацій початкового етапу розслідування шахрайств, вчинених з використанням ЕОТ, два взаємопов'язаних чинники, зокрема: 1) наявність інформації про особу злочинця; 2) спосіб вчинення кримінального правопорушення.

Висновки до розділу 2

Визначаючи основні напрями розслідування шахрайств, учинених з використанням ЕОТ, вказано на необхідність встановлення місця розташування ЕОТ, з якої здійснювалися дії, пов'язані з незаконним заволодінням чужим майном, з подальшим встановленням осіб, які причетні до такого виду шахрайства. Важливим компонентом розслідування вказаних кримінальних правопорушень є проведення процесуальних дій за напрямом заволодіння та використання злочинцем предмета шахрайства.

Важливим компонентом доказування шахрайств, учинених з використанням ЕОТ, відповідно до п. 1 ч. 1 ст. 91 КПК України, є доказування події кримінального правопорушення. Установлення способу вчинення вказаного кримінального правопорушення у перспективі створює передумови для визначення форми вини під час вирішення питання про притягнення особи до кримінальної відповідальності за ч. 3 ст. 190 КК України. Підкреслено, що у кримінальному провадженні про вчинення шахрайств з використанням ЕОТ обов'язково потрібно довести факт усвідомлення підозрюваним (обвинуваченим) кримінально протиправного характеру своїх дій, де винуватість є однією з обставин, які підлягають доказуванню в кримінальному провадженні. З'ясування мотиву кримінального правопорушення є одним з головних завдань під час розслідування кримінальних правопорушень. Зазначено, що відповідно до п. 3 ч. 1 ст. 91 КПК України, у кримінальному провадженні підлягає доказуванню також розмір процесуальних витрат. У межах встановлення обставин, що характеризують особу підозрюваного, становить інтерес інформація, яка безпосередньо не пов'язана з учиненим кримінальним правопорушенням. До таких даних належать відомості про вік особи, стан її здоров'я, поведінку, колишні судимості тощо. Крім того, до суб'єктивних чинників, що визначають такий структурний елемент криміналістичної характеристики, як «особа злочинця», віднесено: наявність у злочинців

попереднього злочинного досвіду, зокрема й знання конкретних способів учинення шахрайства, приховування його слідів, індивідуальні особливості особи злочинця тощо.

Наведено класифікацію типових слідчих ситуацій на початковому етапі розслідування шахрайств, учинених з використанням ЕОТ. Доведено, що найбільш оптимальним критерієм типізації слідчих ситуацій початкового етапу розслідування вказаних кримінальних правопорушень є обсяг і зміст інформації про спосіб учинення кримінального правопорушення та особу, яка його вчинила. За вказаним критерієм слідчі ситуації можна розподілити на чотири групи:

1) 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;

2) встановлено факт шахрайства з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї;

3) інформація про спосіб вчинення шахрайства невідома, а установчі дані про особу злочинця, яка його вчинила – відсутні;

4) за результатами проведених оперативно-розшукових заходів чи аналізу повідомлень у засобах масової інформації було відкрито кримінальне провадження за фактом вчинення шахрайських дій щодо потерпілого, але останній відмовляється співпрацювати з правоохоронними органами як у частині підтвердження самого такого факту, так і подальшого його розслідування. Під час досудового слідства у кримінальних провадженнях щодо шахрайств, учинених з використанням ЕОТ, можуть виникати інші слідчі ситуації. Разом з тим такі типові слідчі ситуації зустрічаються в практичній діяльності поліції вкрай рідко і мають поодинокий характер.

Виокремлено наступні типові загальні версії під час розслідування розглянутих видів кримінальних правопорушень:

1) щодо особи злочинця: а) шахрайство з використанням ЕОТ вчинене

відомою для потерпілого особою або особою, щодо якої є достатньо даних для її встановлення; б) шахрайство з використанням ЕОТ вчинене невідомою для потерпілого особою;

2) щодо механізму вчинення шахрайства: а) шахрайство вчинене особою, яка має поверхневі знання у користуванні ЕОТ; б) шахрайство вчинене особою, яка є спеціалістом у сфері інформаційних технологій;

3) щодо кількості злочинців: а) шахрайство з використанням ЕОТ вчинене одноособово; б) шахрайство з використанням ЕОТ вчинене групою осіб; в) шахрайство з використанням ЕОТ вчинене організованою злочинною групою;

4) щодо співучасників шахрайства: а) особа (виявлений злочинець) має інформацію про інших співучасників (членів групи) і може назвати їх; б) особа (виявлений злочинець) не має інформації про інших співучасників групи, бо останні були одноразово залучені для виконання певної ролі під час вчинення кримінального правопорушення, між собою незнайомі і не є постійними членами організованої злочинної групи; в) особи, що сприяли у вчиненні кримінального правопорушення, не були поінформовані про злочинні дії, не мали наміру заволодіти майном чи правом на майно, а лише виконували дії, які не заборонені законодавством України (наприклад, розробка сайту, надання послуг з його розміщення, розробка програмних засобів тощо);

5) щодо кількості вчинених кримінальних правопорушень: а) шахрайство з використанням ЕОТ вчинене вперше; б) шахрайство з використанням ЕОТ вчинене неодноразово;

6) щодо поширеності шахрайства: а) облежана кількість шахрайств; б) регіональне поширення шахрайського посягання; в) шахрайства вчиняються на державному рівні;

7) щодо місця розташування ЕОТ, з якої злочинці вчиняли контакти з потерпілим: а) особи, які причетні до вчинення шахрайства, використовували ЕОТ, що розташована на території України; б) особи, які причетні до

вчинення шахрайства, використовували ЕОТ, яка розташована за межами території України; в) особи, які причетні до вчинення шахрайства, використовували ЕОТ, розташовану на тимчасово окупованій території у Донецькій та Луганській областях або анексованій Автономній Республіки Крим;

8) щодо мотиву вчинення шахрайства: а) шкоду завдано лише потерпілим, які звернулися з відповідною заявою; б) потерпілих від злочинної діяльності значно більше, але вони не звернулися до правоохоронних органів з різних причин (через сором, що їх ошукали; через незнання, що вчинені зловмисником дії є злочином; через відсутність довіри до правоохоронних органів тощо).

РОЗДІЛ 3
ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ТА ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВ, УЧИНЕНИХ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ

3.1 Проведення невербальних слідчих (розшукових) дій під час розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки

Ефективне розслідування шахрайств, учинених з використанням ЕОТ, насамперед, належить невербальним слідчим (розшуковим) діям, до яких відносяться такі слідчі (розшукові) дії, в результаті проведення яких слідчий, прокурор самостійно отримує інформацію, що знаходиться на об’єктах матеріального світу. Такими слідчими (розшуковими) діями можуть бути обшук, огляд, освідування [155].

Проведення обшуку регламентовано ст. ст. 234–236 КПК України [132]. Зокрема, у ч. 1 ст. 234 КПК України передбачено, що обшук проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб. Доволі важливим є й те, що обшук проводиться на підставі ухвали слідчого судді (ч. 2 ст. 234 КПК України). У ст. 235 КПК України встановлено вимоги щодо ухвали про дозвіл на обшук житла чи іншого володіння особи [132].

Обшук проводиться тоді, коли для цього є підстави, передбачені ст. 234 КПК України. Він може бути проведений не лише у підозрюваного, обвинуваченого, а й в інших осіб, у яких передбачається наявність будь-яких речей, предметів, що мають значення для справи. У підозрюваного він

проводиться в обов'язковому порядку, незалежно від часу вчинення кримінального правопорушення.

Питання проведення обшуку у ході розслідування шахрайств, зокрема учинених з використанням ЕОТ, не нове в літературі з кримінального процесуального права та криміналістики. Істотний внесок у його вивчення зробили відомі вчені України та інших держав: В. П. Бахін, А. Ф. Волобуєв, С. Ф. Денисюк, М. І. Єнікеєв, Н. І. Клименко, О. Н. Колесниченко, В. П. Колмаков, В. О. Коновалова, В. П. Крючков, В. С. Кузьмічов, Є. Д. Лук'янчиков, І. Х. Максутов, С. П. Митричев, Д. О. Турчин, М. В. Салтевський, П. В. Цимбал, В. Ю. Шепітько, І. М. Якимов та ін.

Проте в працях зазначених науковців здебільшого звертається ґрунтовна увага на загальні питання проведення огляду місця події та інші види огляду, їхні методи, способи, стадії, окремі рекомендації щодо характерних місць пошуку певних видів слідів залежно від виду кримінального правопорушення, способу його вчинення. Водночас залишилися недослідженими особливості проведення огляду та обшуку під час розслідування шахрайств, учинених з використанням ЕОТ, що мають свою відчутну специфіку.

Виходячи зі способів вчинення шахрайств, під час яких використовується ЕОТ, варто мати на увазі, що відправлення та передача інформації про предмет шахрайства, а також в окремих випадках спілкування між потерпілим і злочинцем, здійснюються в електронній формі, зокрема за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем.

Саме тому, для виявлення ЕОТ, з якої було здійснено відправлення та передачу інформації, засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, що використовувались з метою вчинення таких видів шахрайств, важливе місце належить обшуку, що сприяє виявленню доказової та орієнтуючої інформації.

Обшук у кримінальних провадженнях про шахрайство, що вчиняється з використанням ЕОТ, має свою специфіку, що визначається самим видом кримінального правопорушення, так як місця обшуку можуть бути різними. Як правило, обшуки у кримінальних провадженнях за фактом шахрайства, учиненого з використанням ЕОТ, здійснюються: за місцем проживання підозрюваного; у місцях, які використовувались підозрюваним для виходу у мережу Інтернет під час вчинення шахрайства; місцях зберігання ЕОТ, яка була використана з метою вчинення шахрайства; осіб, які були причетні до створення та подальшого адміністрування сайтів, які використовувались у подальшому з метою вчинення шахрайства.

Під час його проведення основну увагу приділяють встановленню саме місця вчинення кримінального правопорушення, яке є найбільш інформативним для пошуку матеріальних слідів кримінального правопорушення та виявлення осіб, які мають відомості про обставини розслідуваного або іншого аналогічного кримінального правопорушення (інші потерпілі, свідки, зокрема очевидці тощо). Як правило, об’єктами обшуку є житлові приміщення, які у низці випадків є одночасно і місцем вчинення кримінального правопорушення.

На підготовчому етапі проведення обшуку необхідно встановити:

1) кількість об’єктів, де буде здійснюватись обшук, та їх точну адресу. Наприклад, проведене анкетування працівників НП засвідчує, що порушення вчинення шахрайства з використанням ЕОТ не обмежується одним об’єктом. Особи можуть здійснювати шахрайські дії з використанням ЕОТ з різних об’єктів;

2) точне розташування приміщень, де буде здійснюватись така слідча (розшукова) дія, як обшук;

3) усвідомлювати, які предмети підлягають обшуку;

4) шляхи підходу і способи проникнення до приміщення, що підлягають обшуку;

5) яка кількість осіб, які проживають (працюють) у приміщенні;

6) наявність у будинку чи на подвір'ї собаки та інших тварин;

7) забезпечення цілісності та охорони місця проведення обшуку.

На думку М. В. Салтевського, дані про осіб, що займають приміщення, яке піддане обшуку, необхідні для визначення найбільш вірогідних місць приховування розшукуваних об'єктів з використанням схованок, підготовлених на основі професійних знань, а також визначення складу і кількості учасників обшуку [202, с. 371]. Така інформація дозволить правильно визначити розстановку задіяного особового складу, а також передбачити можливість вчинення протидії СОГ.

Необхідно відмітити, що організація та проведення обшуку у кримінальних провадженнях про шахрайство, що вчиняється з використанням ЕОТ, відрізняються від обшуку, при розслідуванні традиційних видів шахрайств. Це обумовлено небезпекою навмисного знищення інформації, яка зберігається в ЕОТ, як і самої ЕОТ, що має доказове значення, а також необережним поводженням слідчого та інших членів СОГ, які можуть зашкодити інформації, знищити сліди в ЕОТ в результаті неправильного, некваліфікованого поводження з ЕОТ.

Саме тому однією з найважливіших умов підготовчого етапу проведення обшуку безпосередньо на місці ймовірного вчинення шахрайства з використанням ЕОТ є проведення наступних заходів:

– одержання інформації про предмети, які підлягають виявленню: ЕОТ (стаціонарний комп'ютер, ноутбук, сервер тощо); програмне забезпечення та носії інформації, які необхідно вилучати; особу (осіб), підозрюваної у вчиненні шахрайства, її (їх) професійних навичок з володіння комп'ютерною технікою з урахуванням засобів вчинення кримінального правопорушення і способів подолання інформаційного захисту, можливих дій зі знищення інформації та приховування слідів кримінального правопорушення; видів електронної інформації;

– запрошення спеціалістів – експертів комп'ютерно-технічного відділу Експертної служби МВС України чи працівників підрозділу кіберполіції НП України;

– запрошення понятих, при цьому для вказаних цілей бажано запросити в якості понятих осіб, які розуміються на комп'ютерній техніці;

– підготовка відповідних пристроїв і комп'ютерних засобів, які будуть використовуватися для зчитування та збереження вилученої з ЕОТ інформації;

– проведення інструктажу членів СОГ (при цьому особливу увагу варто приділити їхнім діям під час обшуку) та інших учасників обшуку (суворе дотримання встановлених правил поводження з комп'ютерною технікою і носіями інформації, технічно грамотне проведення пошуку доказів, потрібної інформації) [69, с. 16–17].

Таким чином, під час підготовки до проведення обшуку слідчий може доручити оперативним працівникам, як правило, з підрозділу кіберполіції чи карного розшуку, зібрати необхідні відомості про об'єкт та приміщення, де планується здійснити обшук, осіб, які там знаходяться тощо. З метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в обшуку має право запросити відповідних спеціалістів чи працівників підрозділу кіберполіції.

Робочий етап характеризується такими особливостями.

Визначаються, які об'єкти знаходяться поруч, а також послідовність, спосіб і межі обшуку, досліджується весь комплекс питань, які відносяться до обставин місця події, визначається взаємне розташування та взаємозв'язок елементів обстановки, звертається увага на стан предметів, об'єктів, які будуть поруч.

Відразу після прибуття на місце, де буде здійснюватись обшук, необхідно вжити заходів щодо забезпечення збереження інформації на цих носіях інформації, для чого:

– не дозволяти, кому б то не було з осіб, що працюють в цей час або що

знаходяться в приміщенні по інших причинах, торкатися до ЕОТ, а також користуватися телефоном (у разі екстреної і гострої необхідності можна дозволити користуватися телефоном, проте тільки під контролем);

– не дозволяти, кому б то не було вимикати електропостачання ЕОТ;

– не дозволяти нікому і не проводити самому ніяких маніпуляцій з ЕОТ, якщо їх результат заздалегідь невідомий;

– визначити, чи сполучені ЕОТ, що знаходяться в приміщенні (будівлі, комплексі будівель), що оглядається, в локальну обчислювальну мережу. Разом з тим треба мати на увазі, що сервером може бути не один, а декілька комп'ютерів, розташованих до того ж у різних приміщеннях;

– встановити, чи є з'єднання ЕОТ з іншим устаткуванням, зокрема поза приміщенням, де здійснюється обшук;

– визначити, яка операційна система завантажена, які прикладні програми запущені та які дані введені в ЕОТ [108].

При проведенні обшуку місцезнаходження ЕОТ необхідно враховувати:

– імовірність впровадження особами, зацікавленими в приховуванні кримінального правопорушення, заходів по знищенню інформації й інших цінних даних;

– імовірність установки в ЕОТ спеціальних засобів захисту від несанкціонованого доступу, які, не отримавши у встановлений час спеціального сигналу або коду, автоматично знищують всю інформацію, що зберігається на них, або найбільш важливу її частину, що цікавить слідство;

– імовірність установки на ЕОТ інших засобів захисту інформації від несанкціонованого доступу.

Метою обшуку місця вчинення шахрайств, учинених з використанням ЕОТ, є: вивчення і фіксація обстановки місця події; виявлення, фіксація і вилучення слідів кримінального правопорушення та речових доказів; виявлення злочинця та з'ясування мотивів кримінального правопорушення; висунення версій про подію кримінального правопорушення та його

учасників; отримання даних про осіб, які могли знати про вчинення кримінального правопорушення, з метою організації проведення інших слідчих (розшукових) дій [186, с. 25].

Об’єкти обшуку під час вчинення шахрайства з використанням ЕОТ умовно можна поділити на наступні види, а саме:

1) вказують на належність ЕОТ до вчинення кримінального правопорушення:

– ЕОТ (комп’ютери, їх системні блоки);

– периферійні пристрої (монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, джойстики та інше), комунікаційні прилади комп’ютерів і обчислювальних мереж;

– носії інформації (жорсткі диски, флопі-диски, оптичні диски, флеш-пам’ять, зовнішні та внутрішні диски HDD, SSD тощо);

– роздруківка програмних і текстових файлів;

2) вказують на належність певної особи до вчинення кримінального правопорушення:

– електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них;

– відбитки пальців рук на ЕОТ, периферійних пристроях, носіях інформації та інших предметів, які використовувались з метою вчинення шахрайства з використанням ЕОТ;

– предмети, отримані в результаті вчинення кримінального правопорушення (речі, гроші, інше майно).

Залежно від методу обшук може проводитися за різними методиками: концентричний (за спіраллю – від периферії до центру); ексцентричний (за спіраллю – від центру до периферії); фронтальний (дослідження об’єкта засобами, які розташовані в лінію і переміщуються фронтально); за квадратами (приміщення або територія поділяється на квадрати, що обшукуються по черзі); за секторами (за основу береться точка, від якої по колу здійснюється обшук за секторами: від 30º до 45º) [122, с. 336–337].

Під час обшуку необхідно обов'язково здійснювати фотографування та відеозапис, зокрема з використанням фототаблиць. На думку А. Б. Петруніної, позитивним чинником, що багато в чому попереджає можливі спроби вчинення протидії, є використання у процесі обшуку відеозйомки. Її наявність дозволить зафіксувати: по-перше, безпосередньо сам факт виявлення предметів; по-друге, дотримання всіх процесуальних правил проведення слідчої дії і грамотність дій членів слідчої групи [132].

При проведенні відеозйомки порядку обшуку, доцільно фіксувати навколишню обстановку за допомогою фотозйомки з використанням правил вузлової та детальної зйомки. Усі дії з ЕОТ проводяться спеціалістом, який отримав право проведення огляду місця вчинення кримінального правопорушення з використанням ЕОТ, або фахівцем підрозділу кіберполіції. Передусім знаходиться та у подальшому оглядається ЕОТ. При обшуку необхідно звертати увагу на невеликі листки (клаптики, обривки) паперу, які нерідко прикріпляються до цих пристроїв або знаходяться в безпосередній близькості від нього (на них можуть бути записані коди та інші важливі для слідства позначки).

Приступаючи до огляду ЕОТ, слідчий і фахівець, що безпосередньо виконують всі дії на ЕОТ, повинні дотримуватися певних вимог з метою забезпечення виявлення та вилучення речових доказів (слідів пальців рук та об'єктів біологічного походження). До особливостей вказаного етапу необхідно віднести:

– відображення слідів пальців рук потрібно шукати на клавіатурі комп'ютера, маніпуляторі типу «миша», пристроях змінних накопичувачів даних, вимикачах живлення та інших елементах управління засобами обчислювальної техніки (кнопки, пристрої подачі паперу та ін.), шнурах мережі та розетках на робочому місці (столі), де встановлено ЕОТ, і безпосередньо на корпусі пристроїв, що входять до складу комплексу. Якщо злочинному впливу підпадає інформація на змінному носії (накопичувачі пам'яті, CD–ROM та ін.), то машинний носій та його технологічна упаковка

також будуть зберігати на собі відбитки пальців рук злочинця;

– сліди, що утворюються при підключенні апаратури до ЕОТ, систем ЕОТ та їхніх мереж, на якій або за допомогою якої здійснюється несанкціоноване копіювання інформації. У цьому випадку можна виокремити: відбитки пальців рук на корпусі системного блоку ЕОТ, платах та пристроях, що знаходяться всередині блоку, якщо підключення здійснюється зсередини, розняття, за допомогою яких підключається додаткова апаратура;

– виявлення об'єктів біологічного походження (кров, сперма, букальний епітелій, слина, піднігтьовий вміст, кістки і зуби, волосся з цибулиною), які можуть у подальшому слугувати доказами у кримінальному провадженні, а саме на: ЕОТ, периферійних пристроях (принтер, сканер, клавіатура, мишка, багатофункціональний пристрій, блок безперервного живлення, накопичувачі пам'яті, роутер тощо), робочому місці (стіл, стілець, підлога, коврик для миші, інші предмети, що знаходяться поруч), одязі тощо.

У подальшому при працюючій ЕОТ необхідно:

– зафіксувати (відобразити в протоколі обшуку місцезнаходження ЕОТ, що цікавить слідчого, та його периферійних пристроїв, вказавши кожен пристрій (назву, серійний номер, комплектацію: наявність і тип дисководів, мережевих карт, роз'ємів і т. ін.), наявність з'єднання з локальною мережею і (або) мережами телекомунікації, стан пристроїв (ціле або із слідами розтину та ін.);

– визначити, яка програма виконується на момент початку обшуку, при виявленні працюючої програми по знищенню інформації зупинити її і почати обшук (огляд) ЕОТ саме з цього ЕОТ;

– після зупинки виконання програми здійснити вхід в операційну систему для з'ясування, яка програма викликалася востаннє;

– встановити наявність у ЕОТ зовнішніх пристроїв – накопичувачів інформації на жорстких дисках (вінчестері), а також зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність

модему);

– вжити заходів щодо встановлення пароля доступу до захищених програм;

– закрити всі працюючі на ЕОТ програми (необхідно пам’ятати, що некоректний вихід з деяких програм може викликати знищення інформації або зіпсувати саму програму);

– в разі необхідності скопіювати на з’ємний жорсткий диск, який належить територіальним органам чи підрозділам Національної поліції, програми і файли, які стосуються кримінального провадження;

– відключити від мережі ЕОТ і вимкнути модем;

– спеціально зафіксувавши у протоколі обшуку порядок проведення слідчої (розшукової) дії;

– опечатати їх і вилучити разом з магнітними носіями для дослідження інформації в лабораторних умовах;

– при вилученні технічних засобів додаткові периферійні пристрої (принтери, стрімери, модеми, сканери тощо) доцільно вилучати тільки в тому випадку, якщо на них працювали підозрювані або якщо у слідства є питання щодо їх працездатності [68, с. 20–21].

Вищезгадані дії бажано зафіксувати фото-, відеозйомкою.

При непрацюючій ЕОТ необхідно:

– зафіксувати (відобразити в протоколі обшуку місцезнаходження комп’ютерної техніки (серверу), що цікавить слідство, та його периферійних пристроїв, вказавши кожен пристрій (назва, серійний номер, комплектація: наявність і тип дисководів, мережевих карт, роз’ємів та ін.), наявність з’єднання з локальною мережею і (або) мережами телекомунікації, стан пристроїв (ціле або із слідами розтину і т. ін.);

– якщо є потреба, за допомогою спеціаліста та власника (адміністратора) ЕОТ включити його з дотриманням відповідних заходів безпеки та провести копіювання потрібної інформації в порядку, викладеному вище, на з’ємний жорсткий носій, який належить

територіальному органу чи підрозділу НП.

Вилучати потрібно всю ЕОТ і носії інформації (накопичувачі пам'яті – DVD та CD диски, флешкарти, SSD, HDD тощо). Провести ретельний огляд документації, звертаючи особливу увагу на робочі записи операторів, тому що часто саме в цих записах недосвідчених користувачів можна знайти коди, паролі та іншу дуже корисну інформацію. Записати дані всіх людей, що знаходяться у приміщенні на момент приходу слідчої групи, незалежно від пояснення причини перебування їх у даному приміщенні [60, с. 20–21]. Приділяти конкретну увагу відшуканню засобів телекомунікації, за допомогою яких особи здійснювали зв'язок з потерпілим під час вчинення шахрайських дій.

За наявності можливості безпосереднього доступу до комп'ютера і при відсутності усіх небажаних ситуацій, слідчий і фахівець приступають до його огляду, причому вони повинні чітко пояснювати всі свої дії понятим. Необхідно встановити наявність у комп'ютера зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність модему). По можливості необхідно зробити точну інформаційну копію машинного носія. Якщо під час обшуку виявляються інші предмети та документи – вони також обов'язково пред'являються понятим [108].

Дуже важливим етапом у проведенні обшуку є фіксування його результатів, а саме складання протоколу. Належне оформлення джерела фактичних даних, зокрема протоколу процесуальної дії, передбачено ст. 104 КПК України [132]. Відповідно до ч. 1 цієї статті у випадках, визначених цим Кодексом, перебіг і результати проведення процесуальної дії фіксуються в протоколі. Останній повинен містити не лише результати процесуальної дії, а й опис її перебігу.

Відповідно до ч. 3 ст. 104 КПК України протокол складається з:

– вступної частини, яка повинна містити відомості про: місце, час проведення та назву процесуальної дії; особу, яка проводить процесуальну дію (прізвище, ім'я, по батькові, посада); всіх осіб, як присутніх під час

проведення процесуальної дії (прізвища, імена, по батькові, дати народження, місця проживання); інформацію про те, що особи, які беруть участь у процесуальній дії, заздалегідь повідомлені про застосування технічних засобів фіксації, характеристики технічних засобів фіксації та носіїв інформації, які застосовуються при проведенні процесуальної дії, умови та порядок їх використання, а також підстави для проведення обшуку; правове обґрунтування обшуку (посилання на відповідні статті КПК України); відмітка про роз'яснення учасникам обшуку і понятим їхніх прав і обов'язків; умови проведення обшуку (температура повітря, освітлення); час початку і закінчення обшуку;

– описової частини, яка повинна містити відомості про: послідовність дій; отримані в результаті процесуальної дії дані, важливі для цього кримінального провадження, зокрема виявлені та/або надані речі та документи;

– заключної частини, де повинні міститися відомості про вилучені речі та документи і спосіб їх ідентифікації та умови їх фіксації, відображається інформація про додані плани, схеми, малюнки, фотознімки; спосіб ознайомлення учасників зі змістом протоколу; зауваження і доповнення до письмового протоколу з боку учасників процесуальної дії [132].

Описова частина протоколу має містити відомості щодо загальної характеристики місця проведення обшуку, речову обстановку на ньому, його оточення, меж підданої обшуку території. Описуються також шляхи підходу до об'єкту обшуку (у разі потреби), щодо самого місця обшуку – стан входів, суміжних приміщень, сходів, дверей, вікон, замків.

У протоколі предмети описуються послідовно, як були виявлені та оглянуті, та у тому вигляді, в якому знаходилися на момент їх виявлення:

1) розташування місця проведення обшуку та речова обстановка в ньому;

2) опис зовнішнього вигляду приміщення, в якому було виявлено порушення встановлених правил обігу, наявність предметів і речей взагалі, а також інші зміни в обстановці, які були зроблені під час обшуку;

3) опис предметів здійснюється залежно від обраного методу обшуку (концентричний, ексцентричний за секторами, за квадратами, фронтальний).

Детально перераховується кожний предмет, який знаходиться всередині приміщення, та описується у тій послідовності, в якій він був виявлений та оглянутий, і в тому вигляді, в якому він знаходився на момент їх виявлення. Під час огляду предметів описуються його характерні ознаки, а саме, точно вказується місцезнаходження ЕОТ та їх взаємне розташування один щодо одного і навколишніх предметів; описується зовнішній вигляд ЕОТ та її складові частини, порядок з'єднання різних вузлів і деталей між собою з вказівкою наявних особливостей (кольору, штампів, написів і т. ін.); характеризується та індивідуалізується, записуються номер, марка, назви, серії, номер, форма, колір пристроїв; описується порядок з'єднання між собою всіх пристроїв із зазначенням особливостей з'єднання (кількість, розміри, характерні індивідуальні ознаки з'єднувальних проводів, кабелів, шлейфів, розняття); наявні дефекти на пристрої, інші індивідуальні ознаки; всі маніпуляції з ЕОТ та іншими засобами (включаючи натискання клавіш), які зроблені в процесі проведення СРД, їхній результат (наприклад, при копіюванні файлів); встановлюється відсутність або наявність комп'ютерної мережі, телекомунікацій (тип зв'язку, апаратура, що використовується, робоча частота); якщо здійснювалося копіювання інформації – описується яка саме інформація та на який пристрій; вид упаковки.

За можливості (якщо слідчим вдалося це встановити) вказується – конфігурація комп'ютера з чітким описом усіх комплектуючих і пристроїв (наприклад, назва системної плати – ASUS P4P800, виробник процесора – Intel; модель процесора – Pentium G5400; частота процесора 3,7 ГГц; кількість ядер – 2 шт; тип оперативної пам'яті – DDR4; об'єм оперативної пам'яті – 16 ГБ; частота оперативної пам'яті – 2666 МГц; тип накопичувача –

HDD; об’єм накопичувача – 2 ТБ. Відеокарта: виробник відеоплати – nVidia; модель графічного процесора – GeForce GTX 1050Ti; об’єм відеопам’яті – 4 ГБ. Монітор: модель – Samsung C27R500FHIX; діагональ екрану – 42 см; Клавіатура: модель – HyperX Alloy Origins (HX-KB6RDX-RU). Маніпулятор типу «миша»: модель – Logitech G502 Lightspeed Wireless; спосіб під’єднання – бездротовий. Також зазначаються назви моделей і серійні номери кожного з пристроїв, якщо вони нанесені на ці пристрої, де позначками чітко вказано, що це серійний номер – «Serial Number», «Serial N» чи «S/N» та інша інформація із заводських наклейок, а також наявні інвентарні номери, що присвоюються бухгалтерією при постановці обладнання на баланс підприємства (за наявності таких).

У протоколі повинні використовуватися тільки однозначні слова і вирази, які вживаються у сфері комп’ютерних технологій, потрібно уникати жаргонних слів, що позначають згадані предмети, а також незагальновживаних скорочених слів і словосполучень, що використовуються у звичайній мові для позначення комп’ютерної техніки.

Щодо інших предметів: повний перелік усіх вилучених під час вказаної слідчої (розшукової) дії предметів; вид упаковки.

У разі виявлення слідів пальців рук в протоколі обшуку потрібно описати: місце їх виявлення (на яких предметах вони знайдені, де ці предмети знаходилися на місці кримінального правопорушення, назва та призначення предметів); кількість слідів та їх розташування (відстань від двох нерухомих орієнтирів); опис поверхні предмета (скло, папір, метал, деревина, пластмаса, пофарбована, непофарбована, нікельована, полірована, різнокольорова тощо); стан поверхні предмета (суха, волога, маслянiста, забруднена, покрита пилом); вид слідів (потожирові, забарвлені, рельєфні, слабко-видимі, невидимі); при можливості визначення – тип узору (дуговий, петльовий, завитковий); форма та розмір сліду (максимальна довжина та ширина); спосіб виявлення (візуальний, забарвлення порошками або парами йоду і т. ін.); спосіб вилучення при фіксації (сам предмет або його частина

разом зі слідом, фотографування, копіювання на плівку, виготовлення зліпка, матеріал зліпка); як упакований та якою печаткою опечатувались речові докази [122, с. 141].

Під час складання протоколу необхідно звернути особливу увагу на відображення у протоколі конкретного місця вилучення предмета, докладний їх опис, а також на зазначення порядку упакування та опечатування вилученого, скріплення підписами понятих. У разі необхідності складається схема розміщення слідів на тому чи іншому предметі із зазначенням розмірів. Схема розташування виявлених слідів додається до протоколу обшуку.

При необхідності додатково фотографують виявлені предмети та сліди. З цією метою біля кожного предмета розставляються відповідні цифрові бирки та масштабні лінійки (метрики), які свідчать про розмір предметів, при цьому цифри повинні знаходитись біля кожного предмета і не повторятись. Предмети необхідно фотографувати та знімати на відеоплівку у різних ракурсах і положеннях.

Наприкінці протоколу наводяться всі заяви і зауваження понятих і учасників обшуку з приводу тих чи інших дій слідчого. За відсутності зауважень у протоколі робиться відмітка про те, що таких зауважень не надійшло. Обидва примірники протоколу, а також опис вилучених предметів підписують слідчий, особа, у якої проводився обшук, та запрошені особи, які були присутні. Якщо у ході обшуку були зроблені спроби знищити або приховати певні предмети чи документи, що підлягають вилученню, то про це у протоколі робиться відповідний запис й указуються вжиті заходи.

У протоколі потрібно вказати повний перелік всіх вилучених предметів. До протоколу мають додаватися схематичні чи масштабні плани місця події, схеми, фотознімки, відеозапис.

Після опису вилучені предмети та документи упаковуються та опечатуються. Для збереження слідів кримінального правопорушення вилучена ЕОТ опечатується у наступний спосіб: виключити ЕОТ, відключити її від мережі, від’єднати роз’єми і накласти на них лист паперу, закріплюючи

його краї на бокових стінках комп'ютера густим клеєм або клейкою стрічкою для того, щоб виключити можливість роботи з ним у відсутність власника чи експерта. Також необхідно опечатати всі складові ЕОТ паперовими стрічками, на яких ставляться підписи слідчого, спеціаліста, понятих, номер ЕОМ. Для приклеювання використовується липка стрічка, яку кріплять таким чином, щоб при спробі зняти її порушилася б цілісність паперу з підписами. Аналогічно опечатуються роз'єми (кабелів) із додержанням відповідності номерів на рознятті блоку комп'ютера і з'єднувальних проводів.

Магнітні носії поміщаються, зберігаються і транспортуються в спеціальних екранованих контейнерах чи в стандартних дискетних або інших алюмінієвих футлярах заводського виготовлення для того, щоб виключити руйнівну дію різних електромагнітних і магнітних полів і направлених опромінювань. Опечатуються тільки контейнери чи футляри. Пояснювальні надписи наносяться на спеціальні етикетки для дискет.

Інші предмети, які будуть вилучатися, упаковують в окрему тару та опечатуються для подальшого направлення на експертне дослідження. Для упаковки можна використовувати: поліетиленові пакети, паперові чи тканинні мішки, коробки, конверти тощо, які після закладення у них вилученого предмета заклеюються, прошиваються, перев'язуються та опечатуються. На упаковці робляться пояснювальні записи, в яких зазначається: хто, де, коли провів вилучення; у кого воно було проведено; яким чином опечатано вилучене і номер печатки; робиться завірчий підпис співробітника і понятих, а також особи, в якої було проведено вилучення.

Протокол підписується слідчим та іншими учасниками слідчої (розшукової) дії (спеціалістами, понятими, особою, у якої проведено тимчасовий доступ), а також іншими присутніми (представниками адміністрації, технічного персоналу), що мають відношення до роботи ЕОТ (при проведенні СРД у службових приміщеннях).

Обшуку підлягають особи, які знаходяться у приміщенні, та їхні особисті речі. За таких обставин можливе вилучення інших предметів, що

також можуть бути речовими доказами.

Важливе значення під час розслідування шахрайства, що вчиняється з використанням ЕОТ, набуває безпосередній огляд ЕОТ, який здійснюється після її вилучення за результатами обшуку або безпосередньо на місці вчинення кримінального правопорушення під час проведення такої слідчої (розшукової) дії, як тимчасовий доступ до речей та документів, що здійснюється відповідно до ст. ст. 131, 159–166 КПК України [132].

Специфіка огляду ЕОТ передбачає такі підстави: 1) комп'ютерна інформація є специфічним об'єктом пошуку; 2) обстеження ЕОТ та носіїв інформації може набувати самостійного значення; 3) не завжди наявна можливість у вилученні ЕОТ, окремих їх комплектуючих, щоб за допомогою інших дій зафіксувати і дослідити інформацію; 4) обстеження ЕОТ і її носіїв завжди передбачає необхідність запрошення відповідного спеціаліста (у галузі комп'ютерних технологій, комп'ютерних систем тощо); 5) ЕОТ набуває все більшого поширення, й існують різноманітні програми захисту та екстреного знищення інформації [39, с. 76].

Разом з тим перед оглядом ЕОТ рекомендується обов'язково отримати ухвалу слідчого судді на здійснення тимчасового доступ до речей і документів (ст. ст. 159, 164 КПК України) в частині ознайомлення з інформацією та зняття копій такої інформації. Це пов'язано з тим, що під час огляду слідчий (спеціаліст) можуть входити в облікові записи соціальних сторінок, в особистий кабінет інтернет-банкінгу, продивлятись особисту електронну переписку підозрюваної особи тощо.

Приступаючи до огляду, необхідно передбачити обов'язкове проведення відеозйомки та за можливістю фотографування цієї процесуальної дії з метою фіксації послідовності дій слідчого (спеціаліста).

Під час складання протоколу огляду ЕОТ, особливістю його оформлення є необхідність зазначення виду пакувального матеріалу, в якому знаходиться ЕОТ перед проведенням СРД, наявність на пакувальному матеріалі, безпосередньо на ЕОТ та його комплектуючих відповідних пломб,

пломбових стрічок, відповідних печаток, які оформлені належним чином. Одночасно перевіряється, чи є ЕОТ, яка оглядається, безпосередньо тим предметом, який підтягається огляду. Вказане як раз і перевіряється шляхом вивчення пломб і печаток на пакувальному матеріалі ЕОТ, безпосередньо на ЕОТ, а також роз'ємів і місць з'єднань. Це можуть бути наклеєні з аркушу паперу печатки із закріпленням їхніх країв на бокових стінках комп'ютера клеєм або клейкою стрічкою або ж опечатана безпосередньо коробка, целофановий пакет, паперовий чи пластмасовий контейнер, де зберігається ЕОТ. Під час огляду перевіряється, чи відповідає фабула, прізвища, ім'я, по батькові осіб (слідчий, поняті, спеціаліст тощо), та їх підписи, які брали участь у слідчій (розшуковій) дії, під час якої була вилучена ЕОТ, дата проведення такої дії.

Приступаючи до огляду, рекомендуємо слідчому (спеціалісту) здійснити спочатку зовнішній огляд ЕОТ з метою встановлення наступних обставин:

а) склад ЕОТ: наявність системного блоку, монітора, клавіатури, принтера, модему, безперебійного джерела живлення та інших периферійних пристроїв. Якщо це ноутбук – визначення його розмірів. Одночасно встановлюється: тип корпусу, матеріал, з якого він виготовлений, його колір, номер ЕОТ, марка, назви, серія, номер, країна виробник, форма, колір ЕОТ [204]. У разі наявності обов'язково зазначаються індивідуальні ознаки ЕОТ, наприклад, наявність певного малюнку чи начіпки на корпусі, особливий колір, наявність підсвітлювачів на корпусі, неординарний корпус, наявність подряпин, гарантійних наліпок чи інших ознак на корпусі;

б) наявність, кількість і розташування роз'ємів й портів на корпусі для під'єднання зовнішніх пристроїв, а також наявність і види вмонтованих пристроїв, мережевих плат та пристроїв, наприклад, дисководу для гнучких дисків, дисководу для компакт-дисків, відеоплат тощо;

в) встановлення та визначення інших пристроїв, які у подальшому також будуть підлягати огляду з подальшим проведенням їх огляду. Такими

пристроями можуть бути:

– принтер, багатофункціональний пристрій, сканер;

– зовнішні фізичні носії пам’яті HDD, SSD;

– дискові носії – CD, DVD, Blue-Ray-диски, дискети; USB диски;

– флеш-карти пам’яті (SD, micro SD тощо).

Якщо виникла необхідність до підключення периферійних пристроїв чи обладнання до ЕОТ, наприклад, монітору, таке підключення здійснюється з дотриманням відповідних правил.

Після зовнішнього огляду слідчий (спеціаліст) приступають до внутрішнього огляду системного блока. Це пов’язано з необхідністю підтвердження встановлення в ЕОТ пристроїв, плат та іншого обладнання, їх розташування всередині системного блоку. Виявлення нових, не визначених зовнішнім оглядом пристроїв і плат (особливо відмічається наявність невідомих йому пристроїв, наприклад, для знищення інформації). Під час внутрішнього огляду встановлюються індивідуальні ознаки пристроїв і плат, їх серійні номера.

У подальшому включається ЕОТ та фіксуються всі процеси, які відбуваються як у системному блоці, так і на екрані з метою фіксації електронних документів, які знаходяться в ЕОТ. Якщо системний блок вилучався без монітору, то в даному випадку може використовуватися монітор, що належить відповідному експертному підрозділу або правоохоронному органу.

Огляду підлягають наступні фізичні носії ЕОТ:

1) зовнішні фізичні носії пам’яті (жорсткий диск – HDD, SSD; дискові носії – CD, DVD, Blue-Ray-диски, дискети; USB диски);

2) оперативний запам’ятовуючий пристрій ЕОТ (скорочено ОЗП);

3) ОЗП периферійних пристроїв (наприклад, принтер, у пам’яті якого знаходяться документи у «черзі друку»);

4) ОЗП пристроїв зв’язку тощо;

5) флеш-карти пам’яті (SD, micro SD тощо) [103, с. 185].

У разі необхідності з інформації, яка знаходиться в пам’яті ЕОТ, робиться копія на HDD, що належить експертному підрозділу чи правоохоронному органу. Якщо під час огляду ЕОТ виникли проблеми з її запуском, відкриттям і переглядом окремих програм, то в даному випадку здійснюється огляд тих ресурсів (програм, файлів), які дозволяє можливість ЕОТ.

Здійснюючи огляд ЕОТ, які використовувались під час вчинення шахрайства, підлягають огляду наступні види інформації, що стосуються:

– виконуваних у ЕОТ процесів;

– виконуваних сервісів;

– системної інформації;

– даних про користувачів, які перебувають в системі;

– кеш ARP (протоколу визначення адреси);

– кеш DNS (доменної системи імен);

– автоматично завантажених додатків;

– не збережених документів;

– бінарних процесів і сервісів, які зберігаються тільки в оперативній пам’яті [46, с. 21–22].

Так, під час огляду ЕОТ звертається увага та у подальшому відображається у протоколі:

а) електронна переписка, зокрема з потерпілим (коли був створений сайт, його логін і пароль, вихідна та вхідна кореспонденція з потерпілим й інтернет-ресурсами, які були задіяні до вчинення шахрайства;

б) особистий кабінет на сайтах оголошень (наприклад, olx.ua, rst.ua, auto.ria.com/uk/, ab.ua/uk/), зокрема продивляються коли, ким був створений обліковий запис, його назва, логін і пароль, кому належить особистий кабінет, який телефон до нього підключений, коли здійснювалися до нього входження, які повідомлення були розміщені за вказаним обліковим записом, які зміни були здійснені, в який час тощо);

в) здійснюється огляд соціальних мереж, якщо вони підключені до

ЕОТ. Огляду підлягає профіль соціальної сторінки, коли, ким він був створений, його назва, логін і пароль, який телефон до нього підключений, які повідомлення, фотографії, відеоконтент розміщені на профілі тощо;

г) виявляються та оглядаються файли, зокрема фотографії, які були відображенням предмета посягання під час вчинення шахрайства з використанням ЕОТ (наприклад, фотографія транспортного засобу, за який потерпілий сплатив кошти). Ураховуючи, що вказані файли могли були розміщені спочатку на ЕОТ після їх завантаження з телефону чи мережі Інтернет, вони залишають відповідні електронні сліди, а саме дату їх створення або видалення;

д) продивляються особистий кабінет інтернет-банкінгу, коли, ким були вони створені, який у них обліковий запис, на кого вони зареєстровані, їх назва, логін і пароль, кому належить, який телефон до них підключений, які та коли здійснювалися операції по них, зокрема, з отримання коштів від потерпілої особи;

е) оглядаються інші дані, зокрема, назви та версії програм, які встановлені в ЕОТ та можуть бути доказами шахрайства, учиненого з використанням ЕОТ.

Здійснюючи огляд вебсторінки, слідчий повинен її масштабувати у браузері на повний розмір (100 %). У браузері мають бути відключені усі додатки та надбудови, що можуть змінити вигляд вебсторінки, яка оглядається. Основними реквізитами такого електронного документа можуть бути адреса у мережі Інтернет, на якій розміщено вебсторінку; назва вебсайту, категорія чи жанр публікації, якщо вони зазначені на вебсторінці; назва публікації; основний текст публікації; прикріплені зображення та аудіо- чи відеофайли; відомості про автора публікації (якщо публікація не є анонімною) [103, с. 185–186].

У подальшому рекомендується здійснити друк вебсторінок, особистих кабінетів, електронної переписки, профілів в Інтернет-ресурсах, які були предметом огляду, за допомогою службового принтера та додати до

протоколу огляду як невід'ємний додаток, із зазначенням серійного номера, назви та моделі принтера, де друкувалась така інформація [103, с. 188].

Фото-, відео- та аудіофайли, що є частиною публікації, мають бути збережені та записані на диск, який стане другим додатком до протоколу огляду. Альтернативним засобом фіксації вебсторінки є збереження її у форматі html засобами програми-браузера, з подальшим записом такого файлу на диск [103, с. 188].

За результатами огляду може здійснюватись копіювання системи (інформації або даних), яка досліджується, на відповідні пристрої пам'яті (як правило, HDD чи флеш накопичувачі, які належать правоохоронному органу чи експертній установі.

Одночасно всі вказані процедури фіксуються за допомогою фото- та відеозйомки.

Складаючи протокол огляду, зауважимо на певних його складових частинах. Зокрема, у ньому підлягають внесенню наступні дані:

– тип ЕОТ, тип його корпусу, матеріал, з якого він виготовлений, його колір, номер ЕОТ, марка, назви, серія, номер, країна виробник, форма, колір ЕОТ. У разі наявності обов'язково зазначаються індивідуальні ознаки ЕОТ, наприклад, наявність певного малюнку чи начіпки на корпусі, особливий колір, наявність підсвітлювачів на корпусі, неординарний корпус, наявність подряпин, гарантійних наліпок чи інших ознак на корпусі;

– конфігурація комп'ютера з чітким описом усіх комплектуючих і пристроїв (наприклад, назва системної плати – ASUS P4P800, виробник процесора – Intel; модель процесора – Pentium G5400; частота процесора 3,7 ГГц; кількість ядер – 2 шт; тип оперативної пам'яті – DDR4; об'єм оперативної пам'яті – 16 ГБ; частота оперативної пам'яті – 2666 МГц; тип накопичувача – HDD; об'єм накопичувача – 2 ТБ. Відеокарта: виробник відеоплати – nVidia; модель графічного процесора – GeForce GTX 1050Ti; об'єм відеопам'яті – 4 ГБ. Монітор: модель – Samsung C27R500FHIX; діагональ екрану – 42 см; Клавіатура: модель – HyperX Alloy Origins (HX-

KB6RDX-RU). Маніпулятор типу «миша»: модель – Logitech G502 Lightspeed Wireless; спосіб під'єднання – бездротовий. Також зазначаються назви моделей і серійні номери кожного з пристроїв, якщо вони нанесені на ці пристрої, де позначками чітко вказано, що це серійний номер – «Serial Number», «Serial №» чи «S/N» та інша інформація із заводських наклейок, а також наявні інвентарні номери, що присвоюються бухгалтерією при постановці обладнання на баланс підприємства;

– наявність, кількість та розташування роз'ємів і портів на корпусі для під'єднання зовнішніх пристроїв, а також наявність та види вмонтованих пристроїв, мережевих плат і пристроїв, наприклад, дисководу для гнучких дисків, дисководу для компакт-дисків, відеоплат тощо;

– назва інших пристроїв, які у подальшому також будуть підлягати огляду з подальшим проведенням їх огляду. У разі підключення периферійних пристроїв чи обладнання до ЕОТ, які належать правоохоронному органу, зазначається їхня модель, назва пристрою та серійний номер;

– внутрішній огляд системного блока (зазначаються пристрої, плати та інше обладнання, їх розташування всередині системного блоку, вказуються їхні індивідуальні ознаки, серійні номери);

– процеси, які відбуваються як у системному блоці, так і на екрані під час огляду локальних дисків ЕОТ, бінарних процесів і сервісів, а саме:

а) електронна переписка, зокрема з потерпілим (коли був створений сайт, його логін і пароль, вихідна та вхідна кореспонденція з потерпілим й інтернет-ресурсами, які були задіяні до вчинення шахрайства;

б) особистий кабінет на сайтах оголошень (наприклад, olx.ua, rst.ua, auto.ria.com/uk/, ab.ua/uk/), зокрема продивляються коли, ким був створений обліковий запис, його назва, логін і пароль, кому належить особистий кабінет, який телефон до нього підключений, коли здійснювалися до нього входження, які повідомлення були розміщені за вказаним обліковим записом, які зміни були здійснені, в який час тощо);

в) огляд соціальних мереж (сам профіль, коли, ким він був створений, його назва, логін і пароль, який телефон до нього підключений, які повідомлення, фотографії, відеоконтент розміщені на профілі тощо);

г) файли, зокрема фотографії, які були відображенням предмета посягання під час вчинення шахрайства з використанням ЕОТ, опис фотографій та відео, які були предметом шахрайства;

д) особистий кабінет інтернет-банкінгу, коли, ким були вони створені, який у них обліковий запис, на кого вони зареєстровані, їхня назва, логін і пароль, кому належить, який телефон до них підключений, які та коли здійснювалися операції по них, зокрема з отримання коштів від потерпілої особи;

е) назви та версії програм, які встановлені в ЕОТ та можуть бути доказами шахрайства, учиненого з використанням ЕОТ;

є) електронні документи, які розміщені у мережі Інтернет (назва вебсторінки, вебсайту, назва публікації, основний текст публікації, прикріплені зображення та аудіо- чи відеофайли, відомості про автора публікації (якщо публікація не є анонімною) [103, с. 186–188]:

– додатки, які є складовими частинами протоколу огляду (надруковані вебсторінки особистих кабінетів, електронної переписки, профілів в інтернет-ресурсах, які були предметом огляду);

– спосіб знаття копії жорстких дисків, окремих файлів і папок, а також назва пристрою, на який буде здійснено копіювання інформації, його виробничий та інвентарний номер, характеристики, спосіб опечатування;

– наявність біологічних об’єктів і слідів пальців рук на внутрішньому обладнанні та мікросхемах ЕОТ.

Після виконання всіх необхідних вказаних вище дій наприкінці протоколу зазначаються всі заяви присутніх під час огляду та ставляться підписи [103, с. 186–188].

Підводячи підсумки до підрозділу, зазначимо, що обшук та огляд у кримінальних провадження за фактом шахрайства, учиненого з

використанням ЕОТ, є однією з найбільш складних, об’ємних та інформаційно значимих СРД, від якості проведення якої залежить успіх подальшого розслідування кримінальних проваджень. Саме тому дотримання практичних рекомендацій, що наведені вище, з питань проведення обшуку та огляду має важливе значення.

3.2 Проведення вербальних слідчих (розшукових) дій у ході розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки

Однією з найбільш важливих слідчих дій під час розслідування кримінальних провадженнях, пов’язаних з шахрайством, учиненим з використанням ЕОТ, є допит. З метою об’єктивного розслідування зазначених кримінальних правопорушень слідчий допитує підозрюваного, потерпілого та свідків.

Водночас допит – найскладніша слідча (розшукова) дія, що потребує від слідчого високої загальної й фахової культури, глибокого знання психології людини [258].

Проблема допиту учасників кримінального процесу не нова, але вона багатогранна й міждисциплінарна, значна кількість вітчизняних науковців-процесуалістів і криміналістів торкалися різних її сторін з позицій мети своїх досліджень (В. П. Бахін, О. М. Васильєв, Т. В. Варфломєєва, В. К. Весельський, І. Ю. Гловацький, В. С. Комарков, В. О. Коновалова, В. С. Кузьмічова, В. Г. Лукашевич, С. М. Стахівський, В. Ю. Шепітько та інші).

Водночас варто зазначити, що у працях названих учених розглянуто переважно фундаментальні або загальні теоретико-прикладні проблеми, як наслідок, у їх наукових працях не повною мірою висвітлено особливості допиту за вказаним видом кримінального правопорушення.

Допит підозрюваного у кримінальному правопорушенні, передбаченому ч. 3 ст. 190 КК України, здійснюється при дотриманні ст. ст. 224, 276–279 КПК України та інших процесуальних норм, а також з урахуванням відповідних криміналістичних рекомендацій щодо тактики і прийомів провадження цієї слідчої дії, що надає можливість отримати необхідні дані для встановлення винних у його вчиненні осіб, обставини, що характеризують механізм кримінального правопорушення, з'ясувати його детермінанти, обставини вчинення кримінального правопорушення, а також інші факти, що мають значення у кримінальному провадженні. Допит об'єктивно є найбільш поширеною слідчою дією при розслідуванні кримінальних проваджень щодо будь-яких кримінальних правопорушень.

За визначенням В. Ю. Шепітька, допит – це передбачена кримінальним процесуальним законом слідча (розшукова) дія, яка полягає в одержанні слідчим від свідка чи потерпілого, підозрюваного чи обвинуваченого показань про обставини, що мають значення для кримінального провадження [95, с. 372].

У викладенні М. О. Янкового, допит – це регламентований кримінальним процесуальним законом процес специфічної вербальної взаємодії з допитуваним, під час якої слідчий (прокурор, суддя), використовуючи законні практичні прийоми і методи психологічного впливу, отримує від допитуваного та фіксує у протоколі усну інформацію про відомі йому обставини, що мають значення для розслідування кримінального правопорушення [266, с. 190].

Предмет допиту по будь-якому з кримінальних проваджень, передусім, складають загальні дані, а саме: обставини, пов'язані з самою подією кримінального правопорушення (час, місце, спосіб, наслідки тощо); обставини, які встановлюють чи спростовують винність конкретних осіб і мотиви їхніх дій, що впливають на ступінь й характер відповідальності підозрюваного; обставини, які відносяться до характеру та розміру шкоди, нанесеної злочином, тощо [15, с. 20]. До окремих видів допиту належать:

допит свідка, допит потерпілого та допит підозрюваного.

Допит проводиться за місцем проведення досудового розслідування або в іншому місці за погодженням з особою, яку мають намір допитати. Кожний свідок допитується окремо, за відсутності інших осіб. Дана слідча дія не може продовжуватися без перерви понад дві години, а загалом – понад вісім годин на день [132].

Безумовно, запорукою результативності допиту підозрюваного під час розслідування шахрайств, учинених з використанням ЕОТ, є ретельна підготовка до його проведення. Умовно у кримінальних провадженнях цієї категорії систему дій слідчого в цьому аспекті можна поділити на такі етапи: 1) підготовчий; 2) безпосереднє проведення; 3) фіксація отриманих результатів [111].

Своєю чергою, підготовчий етап забезпечує раціональне проведення допиту з позиції належного використання можливостей слідчого. Під час вказаного етапу вирішуються наступні питання:

а) визначення кола обставин, що підлягають з'ясуванню. Для цього перед допитом необхідно ще раз звернутися до матеріалів справи, знову продумати план, проаналізувати версії. Підлягають уточненню дані, що безпосередньо відносяться до предмета допиту, і виявлення джерел, з яких допитуваним стали відомі обставини, факти. При підготовці до допиту потрібно заздалегідь з'ясувати, які докази підтверджують його вину, і систематизувати їх для використання в ході допиту. Іноді буває доцільно скласти перелік питань, що цікавлять слідчого;

б) вивчення особистості допитуваного. Роль у вчиненні шахрайств з використанням ЕОТ (організатор, виконавець, посередник, підбурювач), наявність судимості, риси характеру (хитрість, акторські здібності, вигадливість), сімейний стан, взаємини з родичами та їх відношення до кримінального правопорушення, антисоціальна спрямованість особи, освітній ценз, відношення до вчиненого, психологічний тип, характер взаємин з іншими учасниками кримінального правопорушення. Якщо особа

має судимість, бажано витребувати кримінальні провадження (справи), вироки по яких набули законної сили, і ознайомитися з її поведінкою на допитах [54, с. 96];

в) визначення часу, місця допиту і способу виклику на допит. Таким місцем може бути службовий кабінет слідчого чи інші службові приміщення, місце події, робочий кабінет допитуваної особи чи місце її проживання. Якщо у кримінальному провадженні проходить кілька свідків (потерпілих), обвинувачених (підозрюваних), то тактично важливо визначити черговість їх допиту. Місцем допиту, як правило, є кабінет слідчого. Він повинен бути обладнаний скромно, без відволікаючих увагу предметів. Під час допиту потрібно виключити появу сторонніх осіб, шумові подразники (телефонні дзвінки, радіо). Обстановка в кабінеті повинна розташовувати до відвертої бесіди, сприяти встановленню психологічного контакту з допитуваним [240, с. 184–185]. Оскільки, шахрайства на сучасному етапі переважно вчиняються групами, важливо вірно визначити послідовність допиту підозрюваних. Першими рекомендується допитувати рядових членів групи, характеристика особи яких дозволяє припустити їхню схильність до дачі правдивих показань;

г) створення необхідної обстановки для допиту. Обстановка, в якій проводиться допит, не повинна відволікати допитуваного, заважати йому зосередитися;

д) вивчення обставини вчинення шахрайства з використанням ЕОТ та обставин, які підлягають встановленню під час допиту. Встановлюється, яке відношення має особа, яка буде допитуватися, до цього кримінального правопорушення. Необхідно з’ясовувати, які питання необхідно ставити підозрюваному щодо обставин вчинення кримінального правопорушення;

е) вибір відповідних засобів і прийомів для вирішення конкретних завдань допиту. При цьому можливі два варіанти реалізації слідчим наявної в нього сукупності доказів. Перший – це пред’явлення доказів під час проведення декількох допитів, що послідовно змінюють один одного. Другий

– всієї сукупності зібраних доказів на одному з допитів підозрюваного. Як правило, послідовне пред'явлення системи доказів на низці допитів здійснюється в тих випадках, коли підозрюваний вчинив декілька кримінальних правопорушень, що не дозволяє одночасно з'ясувати обставини протиправної діяльності під час проведення однієї слідчої дії; за відсутності можливості отримання окремих доказів у короткі терміни (наприклад, у зв'язку з міжрегіональним характером вчинення шахрайства);

є) визначення кола учасників допиту, зокрема необхідність залучення спеціаліста та використання консультацій фахівців. У допиті бере участь захисник, у разі необхідності – перекладач, а також педагог, законні представники або родичі – якщо особа, яка допитується, неповнолітня;

ж) підготовка необхідних матеріалів, а також технічних засобів допиту. Вирішення питання, пов'язаного з використанням технічних засобів – звукозапису (відеозапису), що допоможе запобігти даванню неправдивих показань, зафіксувати психологічну реакцію допитуваного на несподівані запитання та пред'явлення доказів [67, с. 287–288].

Як зазначає О. В. Сорокевич, «Застосування звукозапису суттєво змінює умови проведення допиту, впливає на характер поведінки допитуваного. Тільки протокольна форма фіксації показань дає можливість допитуваному вільно й безперешкодно маневрувати ... допитуваний може застосовувати різні способи затягування часу; просто мовчати, поставити зустрічне запитання, зробити відверту заяву, вступити в дискусію із несуттєвого питання, не мотивовано послатися на погане самопочуття, поставити свої умови тощо. Звукозапис повністю виключає або значно ускладнює використання всіх названих способів маскування розгубленості, прагнення ухилитися від питань для виграшу часу й обмірковування відповідей» [218, с. 62]. Мають місце випадки активної протидії слідчому, починаючи від відмови підозрюваного підписати протокол допиту після його складання, закінчуючи заявами про психологічний тиск на нього під час проведення слідчої дії, то в найбільш складних випадках, а також у разі

пред'явлення доказів, неодмінно, при допиті завжди повинен проводитися звукозапис або відеозапис [67, с. 288];

з) складання плану допиту. Слідчий завжди повинен планувати майбутній допит: заздалегідь намічати питання, які повинні бути з'ясовані, порядок їх постановки, порядок пред'явлення речових доказів та інших матеріалів провадження. Найчастіше план намічається в усній формі, рідше – у вигляді коротких начерків. Лише в окремих найбільш складних випадках доцільно складати план детально. План може являти собою не суворий алгоритм певних питань, а розгорнуту перспективу діалогу залежно від інформації, яку повідомляє допитуваний, із зазначенням тактичних прийомів, які передбачається застосувати в ході допиту, формулювання питань і т. ін.

Перед допитом встановлюється особа допитуваного, роз'яснюються його права, а також порядок проведення допиту. У разі допиту свідка він попереджається про кримінальну відповідальність за відмову давати показання і за давання завідомо неправдивих показань, а потерпілий – за давання завідомо неправдивих показань [132].

Особливістю допиту підозрюваного при здійсненні даного провадження є те, що слідчий має у своєму розпорядженні, як правило, набагато більшу кількість доказів, які він може використати долаючи позицію допитаного на заперечення своєї вини. Основними джерелами доказів, які пред'являються допитуваним у даній категорії кримінальних проваджень, є: а) вилучені предмети (ЕОТ, предмет злочинного посягання (кошти чи майно); б) висновки експертиз, якими підтверджується належність зазначених предметів до вчинення кримінального правопорушення; в) протоколи допитів свідків і співучасників, які викривають особу в учиненні кримінального правопорушення; г) інші матеріали провадження.

Враховуючи наукові напрацювання О. М. Стрільціва, пропонуємо під час допиту особи, яка підозрюється у шахрайстві, учиненого з використанням ЕОТ, встановити наступні обставини:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адреса місця фактичного проживання, адреса місця реєстрації;

– чи притягався до кримінальної відповідальності. Якщо так, то за які саме кримінальні правопорушення (злочини);

– чи має з числа друзів осіб, які притягалися до кримінальної відповідальності;

– протягом якого часу вона займається протиправною діяльністю, пов’язаною з шахрайством з використанням ЕОТ;

– що спонукало до вчинення шахрайств з використанням ЕОТ;

– хто придумав та організував протиправну схему шахрайства з використанням ЕОТ;

– як давно особа вчиняє шахрайства з використанням ЕОТ;

– де саме та за які кошти була придбана ЕОТ, яка використовувалась для шахрайства;

– яким чином використовувалась мережа Інтернет у протиправній діяльності;

– які інтернет-ресурси використовувались для розміщення повідомлення з метою подальшого вчинення шахрайства з використанням ЕОТ;

– хто створював інтернет-сайт чи допомагав у його створенні, як познайомились (установчі дані, адреса, телефон таких осіб);

– яким саме інтернет-провайдером користувався та під яким ім’ям («ніком») користувалися;

– яка назва інтернет-сайту, яким користувався для вчинення шахрайства з використанням ЕОТ;

– як часто змінювався інтернет-провайдер і «нік»;

– скільки інтернет-сайтів було створено для організації вчинення шахрайства з використанням ЕОТ;

– на яких типах інтернет-сайтів він зареєстрований;

– з якого місця (об’єкта) та о котрій годині здійснювався доступ до

облікового запису у мережі Інтернет з метою вчинення шахрайства;

– під яким ім’ям (логіном) представлявся під час спілкування з провайдерами інтернет-сервісів;

– яким чином домовлявся з користувачами (потерпілими) з метою вчинення щодо них шахрайських дій;

– який спосіб оплати за придбання коштів або майна був рекомендований підозрюваному (контактний чи безконтактний);

– які інтернет-ресурси використовував для подальшого відтворення протиправної діяльності (назва чату, сайту, номера ICQ, адреси електронної пошти (e-mail));

– яким чином підтримувався подальший зв’язок зі співучасниками (мобільний телефон, ICQ, електронна пошта);

– скільки фактів шахрайства з використанням ЕОТ було вчинено (по кожному факту окремо допитати зі з’ясуванням усіх необхідних обставин);

– яким чином одержувались гроші та майно від вчинення шахрайства;

– яким чином отримувалось майно від шахрайства, його місця зберігання або збуту;

– на чиє ім’я, коли та при яких обставинах відкривався банківський рахунок;

– яким чином проводилась конвертація та легалізація коштів, отриманих від шахрайства;

– яким чином проводилась перевірка надходження грошових коштів, отриманих від шахрайства;

– яким чином проводився розподіл грошей між учасниками шахрайства з використанням ЕОТ та яка саме частка залишалась підозрюваному;

– на які потреби витрачались кошти, здобуті від шахрайства;

– хто був задіяний у якості спільників (детально описати функції кожного з них);

– які методи конспірації використовував підозрюваний з метою непритягнення до кримінальної відповідальності;

– яким чином використовувались пристрої мобільного зв'язку в протиправній діяльності;

– скільки часу підозрюваний користується ЕОТ, яку вилучено;

– хто нею ще користується (користувався);

– скільки ЕОТ він ще має і де вона встановлена [224, с. 39–41].

Наведений приблизний перелік питань, що підлягають з'ясуванню під час допиту підозрюваного у досудовому розслідуванні розглянутої категорії кримінального провадження, не є вичерпним. Залежно від результатів проведених допитів свідків, висновків експертиз тощо з'ясуванню та уточненню підлягатимуть й інші питання.

За результатами узагальнення практичного досвіду встановлено, що під час допиту осіб, які використовували ЕОТ з метою вчинення шахрайства, найчастіше слідчі застосовують такі тактичні прийоми: пред'явлення особі, яку допитують, речових доказів та інших матеріалів провадження, що свідчать про користування нею певною ЕОТ, створення та подальше адміністрування вебпорталом (сайтом), здійснення електронної переписки з потерпілим (або здійснення телефонних переговорів), або спростовують її алібі (95,7 %); оголошення показань інших підозрюваних, потерпілих, свідків (60,1 %); використання суперечностей у самих показаннях допитуваного або з іншими доказами (25,0 %); максимальна деталізація показань з метою виявлення суперечностей (16,3 %); надання пропозиції повторного викладення показань про подію загалом або окремі її обставини (13,7 %); вияв розуміння становища, в якому опинилася особа, яку допитують (12,0 %); переконання в необхідності повідомлення правдивих відомостей (4,7 %); спонукання до каяття шляхом формування внутрішнього протесту проти вчинених дій (2,3 %); інше (0,3 %) (Додаток Б).

Важливо повно і детально зафіксувати показання підозрюваного. Якщо їх видумана частина пов'язана зі спробою перекласти свою вину на співучасника, то ця обставина може бути використана під час допиту останнього, який (після цілком можливого обурення) може перейти від

безконтактного стану та брехні до дачі правдивих показань. У цій ситуації, проведення після допитів співучасників одночасного допиту двох чи більше вже допитаних осіб може бути корисним для з'ясування причин розбіжностей у їх показаннях. На початку такого допиту встановлюється, чи знають викликані особи одна одну і в яких стосунках вони перебувають між собою. Згідно з п. 9 ст. 224 КПК України [132] викликаним особам по черзі пропонується дати показання про ті обставини кримінального провадження, для з'ясування яких проводиться допит, після чого слідчим, прокурором можуть бути поставлені запитання. Особи, які беруть учать у допиті, їх захисники чи представники мають право ставити одна одній запитання, що стосуються предмета допиту.

Під час підготовки до допиту підозрюваного, враховувати наявну інформацію, отриману за результатами проведених попередніх слідчих (розшукових) та негласних слідчих (розшукових) дій щодо особи допитуваних, їх відносини із затриманим, способу життя останніх; обсягу відомостей, які має в своєму розпорядженні або може мати свідок; їх відносини з правоохоронними органами тощо, щоб правильно оцінити правдивість їх показань [83, с. 176–177].

Однак, навіть після викриття за допомогою доказів, підозрюваний має психологічні труднощі, що пов'язані з переходом від неправдивих до правдивих показань. У цей момент необхідно переконати підозрюваного дати правдиві показання, у зв'язку з чим рекомендується: з'ясувати причини та мотиви неправдивих показань і нейтралізувати їх; використати виявлені позитивні якості допитуваного; пояснити зміст положень закону, що містить перелік обставин, які пом'якшують кримінальну відповідальність.

Разом з тим одним з найбільш ефективних тактичних прийомів допиту, спрямованим на викриття неправдивих показань підозрюваного, є максимальна деталізація фактів, які наводить допитуваний. Чим більше неправдивих відомостей повідомить особа, тим її легше викрити, тому що видумані факти неможливо продумати до дрібниць, а тим більше зберегти їх

у пам’яті. Крім цього, питання про дрібні деталі кримінального правопорушення створюють у допитуваного перебільшене враження про інформованість слідчого. Така деталізація необхідна також у випадках правдивих показань про незнайомих підозрюваному співучасників для вжиття заходів по їх встановленню.

Якщо підозрюваний відчує справжню зацікавленість у своїй долі, то це буде самим надійним фундаментом його довірчої позиції та встановлення міцного психологічного контакту на весь період провадження. Тому, намагаючись розкрити злочин, не можна виявляти надмірну поспішність під час допиту.

Важливо визначити технічні засоби, які можна використовувати під час допиту. Згідно з п. 5 ст. 224 КПК України під час допиту може застосовуватися фотозйомка, аудіо- та/або відеозапис. Такі засоби психологічно діють на допитуваного, дозволяють слідчому повністю зосередитися на веденні допиту, використовувати надалі при зміні або відмові від раніше даних показань підозрюваним, встановлення неправдивих показань іншими співучасниками. Про застосування аудіо- та/або відеозапису під час допиту повідомляється підозрюваному та іншим учасникам слідчої (розшукової) дії (захисник, законний представник) до її початку. Згідно зі ст. 104 КПК України, якщо допит фіксується за допомогою технічних засобів, текст показань може не вноситися до відповідного протоколу за умови, що жоден з учасників процесуальної дії не наполягає на цьому. У такому разі у протоколі зазначається, що показання зафіксовані на носії інформації, який додається до нього [132].

Допит потерпілих – найбільш поширене джерело отримання доказів у кримінальних провадженнях про шахрайство, вчинене з використанням ЕОТ. Потерпілі допитуються про обставини шахрайства, прикмети та характеристику предметів злочинного посягання. Оскільки такі особи нерідко відчувають емоційну напругу. Це пов’язано з тим, що потерпілі від шахрайства найчастіше схильні приховувати не тільки окремі факти, що

свідчать про вчинення діяння, а й взагалі приховувати свій статус. У таких ситуаціях доцільно говорити про конфлікт потерпілого і слідчого, здатний прийняти форму суперництва [254, с. 125]. Таке відбувається з різних причин, наприклад при неадекватній оцінці потерпілим обставин вчинення кримінального правопорушення. Причина може полягати також в неправильній оцінці слідчим стану потерпілого та його показань. Як зазначається в науковій літературі, основним засобом подолання несумлінності потерпілого має виступати переконання. Наприклад, Б. В. Шавиркін вказує, що «слідчий повинен прагнути до того, щоб потерпілий вільно і свідомо обрав позицію, спрямовану на надання сприяння у встановленні істини у кримінальній справі» [253, с. 125].

При допиті потерпілого, який прагне приховати свій статус або перешкодити встановленню істини у кримінальному провадженні, доцільно керуватися наступними рекомендаціями: а) проведення короткої бесіди перед початком допиту на сторонні теми; б) з'ясування конкретних мотивів протидії слідству; в) пояснення потерпілому, що його поведінка перешкоджає захисту його ж власних прав та інтересів; г) повторне нагадування про відповідальність за відмову від дачі показань і дачу завідомо неправдивих показань. Звісно ж, подібна інформація, особливо висловлена у формі погрози, може звести нанівець всі зусилля слідчого по створенню довірчих відносин з допитуваним. Тому, на наш погляд, згадку про можливість погіршення становища потерпілого можна використовувати тільки в крайніх випадках.

Водночас під час допиту потерпілого доцільно застосовувати систему прийомів психологічного впливу, запропоновану Ф. М. Сокираном: активізація установок та емоційно-вольової сфери; уточнення умов сприйняття потерпілим фактів події, яка відбулася; постановка запитань, що збуджують або послабляють емоційний стан свідка; нейтралізація негативних якостей особи потерпілого і використання позитивних; заклик до почуття сумління та справедливості [217, с. 72].

Під час допиту потерпілого на початковому етапі розслідування необхідним, насамперед, є з'ясування загальної картини події, яка мала місце, схем вчинення шахрайства, а саме: де, за яких обставин, в який час, та яким чином, через кого відбулося знайомство з підозрюваним (на якому сайті, з якого пристрою); як прийшло повідомлення потерпілому – на телефон чи на електронну пошту; як довго тривала переписка між шахраєм і потерпілим; чи надавав шахрай свій телефонний номер для зв'язку з ним; як злочинець відрекомендував себе, які послуги пропонував, за яку суму; яку мету переслідував потерпілий спілкуючись із шахраєм; яким способом підтримував зв'язок з потерпілим; що конкретно було передано злочинцю (яке майно або скільки коштів), яким чином, яка вартість цих речей, прикмети, фізичні характеристики, наявність документації, що підтверджує знаходження його у власності потерпілого; чи знає особу шахрая; чи зустрічався потерпілий із шахраєм, де, коли, тривалість зустрічей; що обіцяв потерпілому шахрай; що вимагав та отримав від нього; хто був свідком вчиненого шахрайства; причини несвоєчасного звернення до правоохоронних органів.

При допиті потерпілих можливе пред'явлення для впізнання речей, про викрадення яких зроблено заяву. Тому дуже важливо встановити, чи не збереглися у потерпілого певні фрагменти від викрадених об'єктів або об'єкти, аналогічні викраденим, їх фотознімки, чеки, гарантійні талони, ярлики, сервісні книжки, квитанції на придбання товарів тощо. У позитивному випаду ці об'єкти підлягають вилученню та приєднанню до матеріалів кримінального провадження. На подальшому етапі розслідування за умов відшукання викрадених речей та їх впізнання, порівняння із вказаними предметами чи фотознімками допоможе перевірити правильність результатів пред'явлення для впізнання, якщо в ньому виникне сумнів [54, с. 88–90].

Категорії свідків за фактом вчинення шахрайства з використанням ЕОТ відрізняються від звичайного шахрайства тим, що у таких кримінальних

провадженнях свідки класифікуються на очевидців, а також осіб, яким було відомо про обставини шахрайства зі слів потерпілого. В останній групі можуть бути особи, з якими потерпілий міг спілкуватися після вчинення шахрайських дій щодо нього (сусіди, близькі, рідні, знайомі). Тут увагу свідка необхідно спрямувати на давання показань про факти, безпосереднім свідком яких був він сам, і факти, які стали йому відомі від інших осіб. Це сприятиме встановленню повного кола очевидців, а можливо і нових потерпілих.

Також до свідків можна віднести осіб, яким шахрай або співучасники продали чи пропонували купити майно, здобуте злочинним шляхом. Варто мати на увазі, що нерідко продаж майна, отриманого шахрайським способом, відбувається через підставних осіб. При підготовці до допиту та його проведенні важливо враховувати мораль і традиції людей, неформальні відносини між ними, забобонність потерпілих, особливість використання мовних термінів і жестів, прийнятих у допитуваного [54].

Також метою допиту свідка може бути отримання інформації не лише безпосередньо про подію кримінального правопорушення, а й інших відомостей, наприклад, про події, які передували кримінальному правопорушенню, особу злочинця й такі, що можуть бути використані у процесі розслідування для виявлення нових доказів, перевірки та оцінки наявних.

За вимогами п. 1 ст. 224 КПК України кожний свідок допитується окремо, без присутності інших свідків [132].

Під час проведення досудового розслідування за фактом вчинення шахрайства з використанням ЕОТ, як правило, в якості свідків допитують понятих, які брали участь в обшуках та оглядах й інших слідчих (розшукових) діях. У даних осіб на допитах необхідно з’ясувати питання щодо тих фактів, які були зафіксовані за їх присутності, зокрема: чи дійсно у підозрюваних та яким чином були вилучені ЕОТ та/чи інші речові докази (майно, що може належати потерпілому, інші телекомунікаційні засоби, за

допомогою яких могло бути вчинене шахрайство, гроші, документи тощо); що пояснював підозрюваний щодо їх походження та приналежності.

Підводячи підсумки до підрозділу зазначимо, що вказаний порядок і визначені особливості допиту підозрюваного, потерпілого та свідків при проведенні досудового розслідування кримінальних правопорушень за фактом шахрайства, учиненого з використанням ЕОТ, майже повністю відповідають практиці, що склалася, та можуть бути застосовані у ході кримінального провадження.

3.3 Використання спеціальних знань під час розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки

Вміле використання спеціальних знань під час проведення досудового розслідування є запорукою його ефективного завершення. Враховуючи специфіку кримінальних правопорушень, пов’язаних з вчиненням шахрайств з використанням ЕОТ, без застосування цих знань проведення кримінального провадження, на нашу думку, є неможливим взагалі. Ще основоположник криміналістики як науки Г. Гросс наголошував на великій ролі спеціальних знань у встановленні об’єктивної істини, у можливості дослідження «реальних доказів» [63].

Питанням використання спеціальних знань а також методичного забезпечення розслідування окремих видів кримінальних правопорушень, зокрема і шахрайств, що вчиняються з використанням ЕОТ, займалися такі вчені-криміналісти, як Ю. П. Аленін, В. П. Бахін, В. Д. Берназ, Р. С. Бєлкін, С. Ф. Бичков, А. І. Вінберг, А. Ф. Волобуєв, В. К. Гавло, В. Г. Гончаренко, Г. І. Грамович, В. А. Журавель, О. О. Ейсман, Г. Г. Зуйков, А. В. Іщенко, Н. І. Клименко, В. Я. Колдін, О. Н. Колесниченко, В. О. Коновалова, В. С. Кузьмічов, В. В. Лисенко, В. К. Лисиченко, В. Г. Лукашевич,

Є. Д. Лук'янчиков, Г. А. Матусовський, Г. М. Надгорний, М. В. Салтевський, М. Я. Сегай, П. В. Цимбал, В. Ю. Шепітько, К. О. Чаплинський, С. С. Чернявський та багато інших.

Упродовж останніх років проблеми використання спеціальних знань під час розслідування шахрайств та інших кримінальних правопорушень, що вчиняються з використанням ЕОТ, були розглянуті у працях таких українських учених, як: А. І. Анапольська, Г. С. Бідняк, І. В. Головкін, Е. В. Дехтярьов, І. В. Іщук, С. М. Князєв, А. В. Крижановський, О. В. Курман, Т. О. Мудряк, І. О. Мусієнко, Т. В. Охрімчук, Н. В. Павлова, Т. А. Пазинич, І. М. Попов, С. В. Самойлов, Д. Г. Терьохін та ін.

З приводу розуміння поняття «спеціальні знання» науковцями висловлюються різні думки. Для початку відмітимо, що одним з перших криміналістів, який зазначив мету використання спеціальних знань, був Г. І. Грамович, а саме для збирання доказової та орієнтуючої інформації, необхідної для розкриття, розслідування та попередження кримінальних правопорушень, а також розробки тактичних й технічних засобів і методів її збору [61, с. 12].

Так, О. О. Ейсман писав, що спеціальні знання – це знання, які не загальновідомі, не загальнодоступні, не мають масового розповсюдження, якими користується обмежене коло спеціалістів [262, с. 91].

М. Г. Щербаковський та О. А. Кравченко [261] вважають, що метою використання спеціальних знань є отримання доказової та орієнтувальної інформації, необхідної для встановлення істини у кримінальній справі.

Т. В. Авер'янова та Є. Р. Россінська визначають спеціальні знання як систему теоретичних знань і практичних навиків у сфері конкретної науки чи техніки, мистецтва чи ремесла, які отримують шляхом спеціальної підготовки чи професійного досвіду та необхідні для вирішення питань, що виникають у процесі судочинства [263, с. 6].

Н. І. Клименко під спеціальними знаннями розуміє професійні знання, навики і вміння у сфері криміналістичних досліджень, інженерної техніки,

медицини, мистецтва, необхідні для вирішення питань, що виникають під час розслідування та розгляду в суді матеріалів кримінального провадження [101, с. 57].

О. В. Бишевець, вивчаючи питання використання спеціальних знань у доказуванні у кримінальних провадженнях, робить такі висновки: 1) про необхідність застосування спеціальних знань для оптимізації процесу розслідування йдеться вже давно; 2) спеціальні знання – сукупність науково обґрунтованих відомостей окремого (спеціального) виду, якими володіють обізнані особи (експерти і спеціалісти) у різних галузях науки, техніки, мистецтва й ремесла, і яких відповідно до норм кримінального процесуального законодавства використовують для успішного вирішення завдань кримінального провадження; 3) основним завданням використання спеціальних знань у ході проведення СРД є сприяння слідчому у виявленні, закріпленні та вилученні предметів і документів, яке здійснюється шляхом застосування необхідних технічних засобів і способів; 4) метою застосування спеціальних знань є отримання доказів у кримінальних провадженнях, яке досягається спеціалістом шляхом надання допомоги слідчому в застосуванні експертно-криміналістичних методів і засобів при збиранні, вивченні (дослідженні), перевірці, оцінці та використанні доказів; 5) хоча в науці форми застосування спеціальних знань систематизуються за різноманітними критеріями, наразі єдиного наукового підходу до їх класифікації немає [28, с. 192].

Г. С. Бідняк у своїй монографії «Теорія і практика використання спеціальних знань при розслідуванні шахрайств» 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 [31, с. 41–44].

І. І. Когутич пропонує таку дефініцію цього поняття: це така сукупність професійних знань, навичок і вмінь, яка отримана в результаті спеціальної освіти та/або досвіду роботи, відповідає сучасному розвитку певної галузі правозастосування, науки, техніки, мистецтва та ремесла, є достатньою для проведення відповідними суб'єктами компетентного (кваліфікованого) вирішення питань, які цікавлять слідство чи суд в конкретному провадженні [105, с. 113–114].

Наведені та інші положення дозволили сформулювати власну позицію з цього питання, зазначимо, що «спеціальні знання», які використовуються під час розслідування шахрайств, що вчиняються з використанням ЕОТ, – це комплекс знань і навичок, з-поміж яких як окремі правові, так і у вузькій (спеціальній) галузі науки, техніки (зокрема, комп'ютерних технологій, криміналістики тощо), отримані в процесі фахової підготовки та професійної діяльності, якими володіють особи-спеціалісти і відповідно до норм кримінального процесуального законодавства використовують із витратою часу й інтелектуальних зусиль у взаємозв'язку з науково-технічними засобами для успішного виконання завдань кримінального провадження, встановлення вагомих обставин, що мають доказове значення [68, с. 98–103].

У криміналістичній літературі загальноприйнятим є виокремлення процесуальної та непроцесуальної форм використання спеціальних знань [186, с. 105]. Такі форми називають зовнішнім вираженням практичного залучення особи, яка ними володіє, до процесу розслідування

кримінального правопорушення. Наявні й інші класифікації форм використання спеціальних знань під час розслідування.

Так, Л. В. Мединська наголошує, що загальновизнаними є дві процесуальні форми використання спеціальних знань у кримінальному провадженні – судова експертиза та участь спеціаліста під час проведення процесуальних дій [147, с. 279–280].

Що стосується процесуальних форм спеціальних знань, то в даному випадку І. І. Когутич до таких основних форм відносить: 1) безпосереднє використання їх слідчим, прокурором, складом суду під час виконання своїх процесуальних функцій збирання, дослідження та оцінки доказів; 2) участь спеціаліста у провадженні СРД; 3) призначення і провадження судових експертиз. Серед непроцесуальних форм доцільно розглядати: 1) консультативну та довідкову діяльність суб'єктів спеціальних знань; 2) проведення ревізій чи аудиторських дій; 3) участь суб'єктів спеціальних знань в ОРЗ; 4) попередні дослідження матеріальних об'єктів спеціалістами та експертами; 5) результати перевірок за криміналістичними обліками. Цікавою є думка науковця щодо можливості поділу форм використання спеціальних знань у ході проведення СРД на основні та допоміжні, традиційні та нетрадиційні [105, с. 113–114].

До форм використання спеціальних знань, на думку О. О. Закатова, Ю. М. Оропая [81, с. 8], відносяться: 1) безпосереднє використання слідчим спеціальних знань у науці, техніці, мистецтві чи ремеслі; 2) призначення експертиз; 3) призначення ревізій; 4) консультаційна допомога спеціаліста без залучення його до безпосередньої участі в слідчих діях; 5) участь спеціаліста в слідчих діях.

В. С. Давиденко доречно вказує на наступні дві форми використання спеціальних знань. Перша з них визначена кримінальним процесуальним законодавством (судові експертизи, участь фахівців у підготовці та проведенні СРД; друга – не передбачена законом (консультативно-довідкова діяльність фахівців з окремих галузей знань) [66, с. 180].

На підставі наведеного вище, а також аналізу інших наукових джерел можемо констатувати, що до основних форм використання спеціальних знань під час досудового розслідування шахрайств з використанням ЕОТ відносяться: залучення спеціаліста до проведення процесуальних дій та залучення експерта для надання висновків з питань, що виникають під час кримінального провадження – процесуальна форма. Серед непроцесуальних (організаційних) форм найбільш дієвими є консультативно-довідкова та аналітична допомога фахівця у відповідній сфері (насамперед фахівця з питань комп'ютерних технологій).

Участь експерта та спеціаліста прямо передбачена кримінальним процесуальним законодавством та іншими нормативними актами, де у нормах безпосередньо зазначено, що для здійснення цих дій необхідні спеціальні знання [181]. Однак процесуальне становище експерта і спеціаліста істотно відрізняються. Розбіжність у цьому становищі полягає у тому, що спеціаліст надає слідчому лише науково-технічну допомогу під час проведення слідчих (розшукових) дій. Використовуючи свої пізнання у визначеній галузі, він бере участь у виявленні, фіксації, вилученні слідів речових доказів, надає консультативну допомогу тощо при проведенні слідчих (розшукових) дій. Пояснення спеціаліста і висновки, що містяться в них, не мають сили доказів. Експерт же, досліджуючи об'єкти експертизи, дає висновок, що є самостійним джерелом доказів. В постанові ПВСУ від 30 травня 1997 року № 8 «Про судову експертизу по кримінальним і цивільним справам», відмічається, що експертний висновок є одним із засобів доказування і сприяє всебічному, повному, об'єктивному дослідженню обставин справи та прийняттю законних і обґрунтованих судових рішень [183].

Під час розслідування шахрайств з використанням ЕОТ необхідність застосування спеціальних знань виникає практично на кожному етапі кримінального провадження. Виокремимо найважливіші етапи:

– участь спеціаліста у проведенні огляду місця події, обшуку при

розслідуванні шахрайств, що вчиняються з використанням ЕОТ;

– участь спеціаліста у проведенні огляду предметів і документів, які вилучені під час огляду місця події та обшуку, при розслідуванні шахрайств, що вчиняються з використанням ЕОТ;

– участь спеціаліста в організації і проведенні допиту при розслідуванні шахрайств, що вчиняються з використанням ЕОТ.

У ч. 3 ст. 237 КПК України [132] зазначено, що з метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді може запросити спеціалістів. Порядок залучення працівників органів досудового розслідування поліції та Експертної служби МВС України як спеціалістів для участі в проведенні огляду місця події визначається наказом МВС України № 1339 від 3 листопада 2015 р., яким затверджено відповідну Інструкцію [181]. Спеціалістами є: інспектори-криміналісти, старші інспектори-криміналісти, техніки-криміналісти, а в разі утворення секторів техніко-криміналістичного забезпечення слідчих дій – керівники зазначених секторів, які входять до структури відповідних органів досудового розслідування та працівники Експертної служби МВС України у складі спеціалізованої пересувної лабораторії. Спеціалісти можуть надавати консультації під час досудового розслідування шахрайств, учинених з використанням ЕОТ, з питань, що потребують спеціальних знань і навичок, й надавати безпосередню технічну допомогу сторонам кримінального провадження під час досудового розслідування [144, с. 100–105].

До участі в слідчих (розшукових) діях спеціалісти залучаються при: недостатньому оволодінні слідчим прийомами і засобами швидкого та якісного виконання тієї чи іншої роботи, яка вимагає спеціальних знань і навичок; одночасному застосуванні низки засобів криміналістичної техніки; необхідності виконати великий обсяг роботи, яка вимагає спеціальних знань і навичок [133].

Як зазначалося у попередніх розділах, у місцях, де вчиняються такі види шахрайств, є ЕОТ, тому потреба в допомозі спеціаліста-консультанта,

якими, як правило, виступають експерти комп'ютерно-технічного відділу Експертної служби МВС України, виникає на початковому етапі досудового розслідування, коли слідчому необхідно оглянути ЕОТ, насамперед, яка знаходиться в робочому (увімкненому) стані. У цьому випадку спеціаліст повинен надати допомогу: в огляді ЕОМ на стадії її виявлення, у т.ч. встановити в ЕОТ наявність зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність модему тощо); фіксування усіх дій з ЕОТ за допомогою фото- та відеотехніки; здійснення опису екрану та прилеглої обстановки; копіювання наявної в ЕОТ інформації; вжиття заходів щодо встановлення пароля доступу до захищених програм; належного та безпечного вимикання ЕОТ; вилучення, упакування та опечатування ЕОТ, інших носіїв інформації (накопичувачі на жорстких і гнучких магнітних дисках, компакт-диски, DVD-диски, ZIP-дискети тощо) та інших предметів і документів для їх дослідження в лабораторних умовах; способів транспортування (перевезення) вилучених предметів.

При необхідності, надання консультацій слідчому з метою отримання під час опитування чи допиту власника або користувача ЕОТ, що дозволить одержати максимально правдиву інформацію [68, с. 17–20].

Важлива роль спеціаліста також полягає у проведенні ретельного огляду документації, звертаючи особливу увагу на робочі записи користувачів ЕОТ, тому що часто саме в цих записах можна знайти коди, паролі та іншу дуже корисну інформацію.

Під час складання протоколу огляду (обшуку) важлива участь спеціаліста з метою фіксування у документах слідчої дії порядку огляду ЕОТ, здійснених маніпуляцій слідчого чи спеціаліста з нею в процесі проведення слідчої дії з обов'язковим використанням комп'ютерної термінології, зокрема зазначення назв, серії та номерів пристроїв, що вилучаються, наявні на них сліди впливу, дефекти, інші індивідуальні ознаки, конфігурації ЕОТ з чітким описом усіх комплектуючих (за наявності такої можливості) та пристроїв,

назви моделей і серійні номери кожного з пристроїв та іншої інформації із заводських наклейок.

Застосування відеозапису повинно забезпечити найбільш точну і повну фіксацію фактів, що мають доказове значення. Відповідно до ч. 7 ст. 236 КПК України під час обшуку відеозапис дає змогу фіксувати не тільки предмети, які підлягають вилученню, а й житло чи інше володіння особи; саму особу; понятих, які присутні при проведенні цієї слідчої дії; слідчого, оперуповноважених. Вказане певним чином дисциплінує їхні дії та відповідність чинному законодавству.

Окрім огляду, важлива роль спеціаліста під час розслідування шахрайств, що вчиняються з використанням ЕОТ, проявляється у наданні слідчому консультацій. Так, предметом консультації з спеціалістом у галузі комп'ютерних технологій може бути:

а) визначення способу та механізму використання ЕОТ під час вчинення шахрайства;

б) з'ясування ступеня належності того чи іншого предмеа, який належить до ЕОТ, в механізмі вчинення шахрайства;

в) способи використання ЕОТ у механізмі вчинення шахрайства;

г) порядок збереження вилучених ЕОТ;

д) можливість використання певного виду технічних засобів для вчинення шахрайства.

Предметом консультації з спеціалістом у галузі фінансово-кредитних операцій може бути:

а) з'ясування виду реквізиту і ступеня належності того чи іншого документа до фінансово-кредитної операції;

б) механізм руху документів і фіксація їх у кредитних установах;

в) порядок збереження документів та умови їх отримання;

г) можливість використання технічних засобів для одержання чи виготовлення документів [20].

Спеціаліст у галузі бухгалтерського обліку може надати консультації з

приводу: процедури руху грошових коштів; документального фіксування і обліку фінансових операцій; бухгалтерської звітності; підбору необхідних для пред'явлення документів тощо [133].

Ще однією формою застосування спеціальних знань у справах про злочини вказаної категорії є залучення спеціалістів до участі у проведенні окремих слідчих дій, зокрема:

– спеціаліста у галузі комп'ютерних технологій для участі в допиті підозрюваного, а іноді – свідка;

– спеціаліста-бухгалтера, економіста, фінансиста або фахівця у галузі комп'ютерної техніки для обшуку або тимчасового доступу до фінансово-бухгалтерської документації;

– спеціаліста у галузі почеркознавства, документознавства для участі в огляді документів – речових доказів тощо.

Спеціаліст не тільки вирішує задачі з виявлення та фіксації факту шахрайства з використанням ЕОТ, вилучення речових доказів, але й допомагає слідчому вирішувати загальні задачі, спрямовані на встановлення всіх фактичних обставин, що характеризують об'єкт і предмет, об'єктивну і суб'єктивну сторони вказаного кримінального правопорушення та його суб'єкта.

Спеціаліст допомагає слідчому скласти протокол проведення слідчої (розшукової) дії. Він консультує його щодо специфічних комп'ютерних термінів, які можуть використовуватись в ЕОТ, допомагає скласти фрагменти протоколу цієї слідчої (розшукової) дії, в яких мова йде про виявлені носії слідів, із вказівкою на їх розташування, типову приналежність, способів фіксації і вилучення, використаної криміналістичної техніки. Вказаний спеціаліст відповідно до ст. 71 КПК України має право вимагати від слідчого занесення до протоколу своїх зауважень і заяв, пов'язаних з виявленням, закріпленням і вилученням доказів [132].

Найбільш процесуально цінною формою використання спеціальних знань у кримінальному судочинстві є призначення судових експертиз. Не

виключенням є розслідування шахрайства, що вчиняється з використанням ЕОТ, де призначення судової експертизи є обов'язковою та найбільш інформативною формою застосування спеціальних знань.

Загальний процесуальний порядок залучення експерта та призначення і проведення експертиз регламентується ст. ст. 69, 70 та 242–245 КПК України [132], Законом України «Про судову експертизу» від 25 лютого 1994 року [182], а також іншими нормативно-правовими актами [89, 174]. Згідно із Законом України «Про судову експертизу» судова експертиза – це дослідження експертом на основі спеціальних знань матеріальних об'єктів, явищ і процесів, які містять інформацію про обставини кримінального правопорушення [182]. Подібним чином визначають судову експертизу в криміналістичній літературі [120, с. 340].

Згідно з кримінальним процесуальним законом експертиза проводиться експертом за зверненням сторони кримінального провадження або за дорученням слідчого судді чи суду, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання. У разі необхідності отримання зразків для проведення експертизи згідно з вимогами ст. 245 КПК України [132] вони відбираються стороною кримінального провадження, яка звернулася за проведенням експертизи або за клопотанням якої експертиза призначена слідчим суддею. У випадку, якщо проведення експертизи доручено судом, відібрання зразків для її проведення здійснюється судом або за його дорученням залученим спеціалістом.

У кримінальних провадженнях про шахрайства криміналісти вважають за доцільне призначати різного роду експертизи: почеркознавча експертиза, технічна експертиза документів, комп'ютерно-технічна експертиза (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення), економічні експертизи [31, с. 78–105]; судово-економічна експертиза; судово-бухгалтерська експертиза; техніко-криміналістична експертиза документів (для виявлення ознак підробки), трасологічна (для встановлення цілого за частинами); експертиза матеріалів,

речовин і виробів (для виявлення на предметах-носіях мікрочастинок або мікрослідів клейких речовин), судово-почеркознавча експертиза [104, с. 143–146].

Вивчення результатів кримінальних проваджень щодо шахрайств, які вчиняються з використанням ЕОТ, надало змогу визначити 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).

Відносно осіб, які є підозрюваними у шахрайстві з використанням ЕОТ, може проводитись судово-медична, судово-психіатрична, дактилоскопічна експертизи.

Залежно від обставин кримінального провадження можуть проводитись інші види експертиз.

Експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза). Згідно з ч. 1 ст. 242 КПК України [132] експертиза проводиться експертом за зверненням сторони кримінального провадження або за дорученням слідчого судді чи суду, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання.

Експертиза комп'ютерної техніки і програмних продуктів призначається у тих випадках, коли необхідно встановити фактичні дані, що мають значення для кримінального провадження і пов'язані із застосуванням комп'ютерної техніки, та вчинені за її допомогою певні дії, які встановлюються на основі спеціальних знань у галузях обчислювальної техніки та програмування.

Порядок надання об'єктів для експертного дослідження, а також проведення їх експертизи регламентовано наказом Міністерства юстиції України від 8 жовтня 1998 р. № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» [89] зі змінами та доповненнями.

У постанові про призначення експертизи слідчий має вказати тип ЕОТ, тип його корпусу, матеріал, з якого він виготовлений, його колір, серійний номер ЕОТ, марку, серію, номер, країну-виробника, форму, колір ЕОТ та її індивідуальні ознаки (наявність певного малюнку чи начіпки на корпусі, особливий колір, наявність підсвітлювачів на корпусі, неординарний корпус, наявність подряпин, гарантійних наліпок чи інших ознак на корпусі тощо). Також необхідно зазначити наявність, кількість та розташування роз'ємів і портів на корпусі для під'єднання зовнішніх пристроїв, а також наявність та види вмонтованих пристроїв, мережевих плат і пристроїв, наприклад, дисководу для гнучких дисків, дисководу для компакт-дисків, відеоплат тощо. Коротко описується спосіб та обставини вчинення шахрайства з використанням ЕОТ. Якщо відомі захисні системи (логін, пароль тощо), обов'язково вони зазначаються. У разі підключення периферійних пристроїв чи обладнання до ЕОТ, які належать правоохоронному органу, зазначається їхня модель, назва пристрою та серійний номер [224, с. 55–56].

До основних завдань експертизи комп'ютерної техніки і програмних продуктів під час досудового розслідування шахрайств, що вчиняються з

використанням ЕОТ, належать:

– установлення робочого стану комп'ютерно-технічних засобів;

– установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

– виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

– установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку [89].

Об'єктами комп'ютерно-технічної експертизи у кримінальних провадженнях за фактом вчинення шахрайства з використанням ЕОТ є:

– електронно-обчислювальна техніка (системні блоки комп'ютерів, ноутбуки, планшети, айподи, сервери, стільникові телефони тощо та їх комплектуючі);

– периферійні пристрої, які використовувались під час виходу ЕОТ в Інтернет-мережу (зовнішні модеми, адаптери комп'ютерних мереж, перемикачі, маршрутизатори, комутатори, стільникові телефони, супутникова телефонія тощо);

– носії інформації (накопичувачі на жорстких оптичних і лазерних дисках (CD, DVD, Blue-ray), комп'ютерні дискети, оптичні компакт-диски, флеш-картки пам'яті, HDD та SSD бокси тощо);

– електронні записні книжки, планшети та інші електронні носії текстової або цифрової інформації [224, с. 56].

Для дослідження робочого стану ЕОТ експерту надають ці засоби, а також технічну документацію до них (за наявності); для встановлення відповідності програмних продуктів певним параметрам – надають носій з копією досліджуваного програмного продукту або програмного коду [224, с. 56].

Для дослідження інформації, що міститься на комп'ютерному носієві, експерту надається цей носій, а за потреби – комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій інформації [224, с. 56].

З метою визначення, які саме об’єкти потрібно надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта або спеціаліста в галузі комп’ютерної техніки [224, с. 56].

До об’єктів, які направляються на комп’ютерно-технічну експертизу у кримінальних провадженнях за фактом вчинення шахрайства з використанням ЕОТ, встановлено такі вимоги:

– для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях;

– системний блок комп’ютера та інші пристрої мають бути упаковані й опечатані в такий спосіб, що унеможливлює їхнє пошкодження, безпосередній доступ до носіїв інформації та підключення системного блока до мережі електроживлення;

– у постанові про призначення експертизи повинні бути точно вказані місце, час вилучення, а також зовнішній вигляд пристроїв і програмних продуктів, які направляються на експертизу;

– при вилученні комп’ютерів та електронних носіїв інформації їх варто упаковувати в поліетиленовий (або полотняний) пакет, який опечатують. Носії інформації можна упакувати в картонну чи пластмасову коробку та опечатати її. Варто зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їхня кількість). Коробку з носіями та опис поміщають до поліетиленового пакету, який заклеюють;

– під час перевезення комп’ютерних засобів вживають заходів щодо запобігання їх механічного пошкодження і взаємодії з хімічно активними речовинами [224, с. 56–57].

Інструкцією про призначення та проведення судових експертиз та експертних досліджень, затвердженою наказом Міністерства юстиції України від 8 січня 1998 р. № 53/5 [89], визначено орієнтовний перелік вирішуваних комп’ютерно-технічною експертизою питань:

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, невстановлене) програмне забезпечення?

Які функціональні несправності мають дане комп’ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання загалом?

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? [89].

Експертиза телекомунікаційних систем і засобів. Об’єктами експертизи телекомунікаційних систем і засобів у кримінальних провадженнях щодо шахрайств, учинених з використанням ЕОТ, є:

телекомунікаційні системи (наприклад, системи мобільних операторів зв’язку, телевізійні системи, радіосистеми тощо);

мобільні термінали (наприклад, телефони, смартфони, планшети та інші мобільні пристрої із встановленим програмним забезпеченням;

білінгові системи (наприклад, білінгові системи мобільних операторів, білінгові системи банків, системи державних реєстрів тощо);

спеціалізовані технічні пристрої (наприклад, станції активних перешкод, телематичні модулі, пульти керування доступом, програматори активних ключів для автомобілів та іммобілайзерів тощо) [96];

Інтернет IP-вузли;

доменні імена, вебсторінки, адресація в мережі Інтернет;

передавачі радіосигналів;

приймачі радіосигналів;

вузли комутації;

первинні мережі зв'язку;

наземні станції супутникового зв'язку [160];

периферійні пристрої, які використовувались під час виходу ЕОТ в Інтернет-мережу (зовнішні модеми, адаптери комп'ютерних мереж, перемикачі, маршрутизатори, комутатори, стільникові телефони, супутникова телефонія тощо).

Основними завданнями експертизи телекомунікаційних систем і засобів є:

– визначення характеристик і параметрів телекомунікаційних систем та засобів;

– встановлення фактів і способів передачі (отримання) інформації в телекомунікаційних системах;

– встановлення фактів і способів доступу до систем, ресурсів та інформації у сфері телекомунікацій;

– визначення якості надання телекомунікаційних послуг на рівні їх споживання;

– встановлення конфігурації та робочого стану телекомунікаційних систем і засобів;

– встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем і засобів;

– дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій [89].

Інструкцією про призначення та проведення судових експертиз та експертних досліджень, затвердженою наказом Міністерства юстиції України від 8 січня 1998 р. № 53/5 [89], визначено орієнтовний перелік вирішуваних експертизою телекомунікаційних систем і засобів питань:

Які тип, марка, модель телекомунікаційного засобу (системи)?

Чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт)?

Які характеристики підключень до мережі має телекомунікаційний засіб?

Чи змінювались користувачем телекомунікаційної мережі налаштування окремих пристроїв, у який час, які їх значення?

Який загальний характер підключень до телекомунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб)?

За допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі?

Яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему?

Чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації?

Які технічні характеристики (параметри) має телекомунікаційний засіб (система)?

Чи мав місце факт доступу до телекомунікаційної системи та в який спосіб?

Чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб?

Чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб?

Чи є ознаки втручання в роботу телекомунікаційної системи?

Чи могли апаратні засоби об’єднуватись у телекомунікаційну мережу та за якими ознаками?

Які шляхи маршрутизації даних у телекомунікаційній системі?

Чи можливо використання телекомунікаційного засобу (обладнання) для вказаних цілей? [89].

При призначенні телекомунікаційної експертизи особливу увагу варто приділяти збору об’єктів дослідження. Найменша некваліфікована дія з телекомунікаційною системою часто закінчується безповоротною втратою цінної розшукової та доказової інформації. У зв’язку з цим для збору об’єктів доцільним є залучення фахівця. Зазвичай сучасні смартфони та планшети мають різні ступені захисту (код доступу, графічний код, відбиток пальця, сканер обличчя тощо) та постійне підключення до мережі Інтернет (інформація, яка в них міститься, може бути заблокована або видалена віддалено). У таких випадах мобільний телефон, смартфон чи планшет необхідно перевести у «авіа-режим» та, при можливості, вилучити сім-карту не вимикаючи його й підтримувати пристрій у розблокованому стані до моменту передачі спеціалісту [96].

Також до типових завдань експертизи належить дослідження білінгових даних мобільного оператора. У сфері телекомунікацій білінг офіційно називається – автоматизована система розрахунків. Як правило, такі дослідження спрямовані на аналіз даних, що фіксують білінгові системи операторів мобільного зв’язку, до яких відносяться наступні дані:

– дата та час з’єднань конкретних абонентів;

– тип з’єднання (телефонний виклик, відправлення або отримання повідомлення від іншого абонента, отримання службових повідомлень тощо);

– місцезнаходження базової станції оператора мобільного зв’язку в момент з’єднання та азимут направлення відповідної антени базової станції.

До завдань, що вирішуються при вказаних дослідженнях, відносяться:

встановлення приблизного місця, де знаходився мобільний термінал під час таких з'єднань, кількість та дата і час з'єднань між певними абонентами, підтвердження факту з'єднання між конкретними абонентами чи групами абонентів тощо. Також проводяться дослідження технічних аспектів функціонування автоматизованої системи розрахунків мобільних операторів, наприклад, підтвердження факту надання послуги абоненту та обсягу послуги і т. ін. [96].

Молекулярно-генетична експертиза. Якщо під час проведення слідчих (розшукових) дій вилучаються предмети, (ЕОТ, їх складові частини (клавіатура, комп'ютерна миша), накопичувач пам'яті (флешка), килимки для комп'ютерної миші, телефони тощо, на яких можуть міститися біологічні сліди, то молекулярно-генетична експертиза забезпечує встановлення наявності, видової і групової належності об'єктів людського походження, які можливо були залишені особами під час користуванням ЕОТ при вчиненні шахрайства.

До об'єктів біологічного походження, які досліджують у лабораторії біологічних досліджень та обліку ДНДЕКЦ МВС України при проведенні молекулярно-генетичної експертизи, належать: кров, сперма, букальний епітелій, слина, піднігтьовий вміст, кістки і зуби, волосся з цибулиною.

Завданням молекулярно-генетичної (ДНК) експертизи є установлення генетичних ознак людини в об'єктах біологічного походження. Методи ДНК-аналізу при дослідженні об'єктів біологічного походження застосовують для встановлення статевої належності та ідентифікації особи. Завдяки цьому вирішується низка питань, що мають значення для розкриття шахрайства, учиненого з використанням ЕОТ.

У ході проведення експертизи вирішуються такі запитання, як:

Чи на представлених об'єктах сліди біологічного походження (слина)?

Кому належать виявлені об'єкти: людині чи тварині? Якщо сліди належать людині, то яка їх групова приналежність?

Кому з осіб, які проходять у кримінальному провадженні, можуть належати виявлені сліди? [73].

Експертиза слідів рук (дактилоскопічна експертиза). Головним завданням дактилоскопічної експертизи є ідентифікація особи за слідами її рук, що залишені на місці події та безпосередньо на ЕОТ, засобах комунікації та інших предметах, яких могли торкатися підозрювані під час вчинення шахрайства з використанням ЕОТ. Якщо версія про особу, що залишила слід, ще не висунута, а також якщо слідчий вважає за потрібне встановити, чи є на предметах обстановки місця події невидимі або слабовидимі сліди, перед експертом потрібно поставити питання про наявність такого роду слідів і їх придатність для ідентифікації особи [89].

Об’єктами дактилоскопічної експертизи є речові докази, на яких знайдено сліди рук або припускається їх наявність. Ними можуть бути сліди пальців та (або) долонь. Експертиза може бути проведена також шляхом дослідження копії сліду на слідокопіювальній плівці, зліпка об’ємного сліду або масштабного фотознімка сліду [89].

Як порівняльні зразки надаються відбитки нігтьових фаланг пальців або відбитки долонь осіб, які підлягають перевірці.

Орієнтовний перелік вирішуваних дактилоскопічною експертизою питань:

Чи є на об’єкті сліди рук?

Чи придатні дані сліди для ідентифікації особи?

Чи залишені сліди рук конкретною (однією) особою?

Чи залишені однією особою сліди рук, вилучені в різних місцях?

Чи є на даному предметі сліди рук і якщо так, то чи придатні вони для ідентифікації?

Якою рукою і якими пальцями руки залишено сліди?

Які особливості мають руки людини, що залишила сліди (відсутність пальців, наявність шрамів тощо)?

Якими ділянками поверхні долоні залишено сліди?

У результаті якої дії залишено слід (захват, торкання тощо)?

Чи були сліди до вилучення на поверхні конкретного об’єкта?

Чи є ознаки переносу вилучених слідів з однієї поверхні на іншу? [89].

Об’єкти дактилоскопічної експертизи мають надсилатися експерту в якомога коротші строки. До кола осіб, що перевіряються, потрібно включати і тих, що не причетні до вчинення кримінального правопорушення, якщо вони могли залишити сліди на місці події. Установлення того факту, що слід залишила певна особа, виключить пошук нових підозрюваних і призначення зайвих експертиз. Якщо в процесі слідчого огляду не було встановлено, якою частиною руки залишено слід, слідчий направляє експерту як порівняльні зразки відбитки всіх трьох фаланг пальців рук підозрюваної особи, а також відбитки долонь [224, с. 59].

Експертиза матеріалів та засобів звукозапису. Така експертиза проводиться з метою дослідження записів дій та переговорів осіб, причетних до шахрайства, або відео-, звукозаписів, здійснених під час здійснення вчинення безпосередньо особою кримінального правопорушення (наприклад, купівлі/продажу (передачі/отримання) предмету шахрайства) з метою встановлення дослівного змісту розмов та ідентифікації особи. Об’єктом дослідження може бути записи дій та переговори осіб, причетних до вчинення шахрайства, з використанням ЕОТ. Експертиза також вирішує питання встановлення технічних умов та технології отримання відеозвукозапису, а також ототожнення особи за фізичними параметрами голосу [89].

Технічна експертиза документів. В окремих випадках способами змінення документів під час вчинення шахрайства з використанням ЕОТ є монтаж із застосуванням копіювально-розмножувальної та комп'ютерної техніки записів, заміна окремих частин документів, у яких відображаються операції з купівлі/продажу окремих видів предметів [89]. Таким чином об’єктом дослідження може бути:

– документи, що засвідчують особу, подію, освіту, трудовий стаж (паспорт; свідоцтва про народження, одруження і розірвання шлюбу, переміну прізвища, імені, по батькові; трудова книжка та вкладиш до неї; посвідчення водія, службові, військові, ветеранів, інвалідів; дипломи про освіту, присвоєння звання; пенсійна книжка; пенсійні листки; листи тимчасової непрацездатності тощо);

– проїзні документи (квитки на проїзд залізничним, морським, річковим, повітряним і міським транспортом; документи на перевезення вантажів тощо);

– документи, що обслуговують грошовий обіг (книжки ощадні, чекові, депозитні; чеки грошові, майнові, розрахункові; бланки фінансування, страхування; акредитиви; марки податкові, митні, акцизні; доручення на видачу коштів, пенсій, майна; сертифікати якості, на право вивезення та ввезення, поліси страхування; ліцензії тощо);

– білети тиражних та миттєвих лотерей;

– цінні папери (акції, облігації, казначейські зобов’язання, ощадні сертифікати, приватизаційні папери, векселя тощо);

– інші документи та цінні папери, передбачені чинним законодавством;

– слідоутворюючі поверхні засобів письма та інших технічних засобів (друкарських форм, печаток, штампів тощо), за допомогою яких виготовляються документи та їх реквізити на певних матеріальних носіях;

– зміст документів (текст, підписи, відбитки печаток, штампів тощо) [76].

Саме тому в окремих випадках виникає необхідність у проведенні технічної експертизи документів. Основними завданнями експертизи друкарських форм з метою установлення типу та ідентифікація комп’ютерної і копіювально-розмножувальної техніки за виготовленими за їх допомогою матеріальними документами [89].

Основними завданнями експертизи матеріалів документів є: установлення роду, виду (іншої класифікаційної категорії) матеріалів, на яких і за допомогою яких виконувався (виготовлявся) документ (папір, барвники, клейкі речовини тощо), та їх спільної (різної) родової (групової) належності; визначення абсолютного часу виконання штрихів рукописних записів у документах. За допомогою технічної експертизи документів можна з'ясувати, зокрема:

Чи замінювались у документі (договорі, зошиті, книзі, медичній картці тощо) аркуші?

Яким чином виконаний підпис від імені особи (прізвище, ім'я, по батькові), текст документа (за допомогою технічних засобів чи писальним приладом)?

Чи виготовлені (виконані) дані документи (фрагменти документа) у різний час?

У якій послідовності виконувались реквізити даного документа (підпис, відтиск печатки тощо)?

Чи виготовлено наданий документ шляхом монтажу за допомогою комп'ютерної або копіювально-розмножувальної техніки?

Який (які) спосіб (способи) поліграфічного друку використано під час виготовлення даного документа?

Яким способом (з використанням набору друкарського шрифту, шляхом рисування тощо) виготовлена дана друкарська форма?

Чи відповідає даний цінний папір (акція, облігація, сертифікат, вексель тощо) за своїми характеристиками аналогічним цінним паперам, що виготовляються Держзнаком України (або вказати іншого виробника)?

Який тип принтера (копіювального апарата, багатофункціонального пристрою), на якому виготовлений наданий документ?

Чи виготовлено наданий документ за допомогою принтера (копіювального апарата, багатофункціонального пристрою), зразки друку якого надані для порівняльного дослідження?

Чи виготовлені надані документи на одному або різних принтерах (копіювальних апаратах, багатофункціональних пристроях)?

Яким способом нанесений відтиск печатки (штампа, факсиміле)? [89].

Предметом експертиз документів бухгалтерського, податкового обліку і звітності є фактичні дані про допущені правопорушення економічного характеру, зокрема, коли шахрайство вчиняється з використанням ЕОТ, яка належить юридичній особі або фізичній особі-підприємцю [47, с. 540]. При цьому необхідно пам'ятати, що проведення ревізійних дій (визначення експертами-економістами будь-яких економічних показників без попереднього проведення документальних перевірок фінансово-господарської діяльності суб'єктом контролю) не належить до завдань економічної експертизи. Сутність експертизи документів бухгалтерського, податкового обліку і звітності передбачає дослідження документів бухгалтерського, податкового обліку і звітності, дослідження документів, що відображають проведення фінансово-кредитних операцій, а також економічної діяльності суб'єкта господарської діяльності, який вчиняє певні шахрайські дії. До завдань цієї експертизи відносять документальне обґрунтування: розміру нестачі або надлишків грошових коштів, періоду і місця їх утворення; відображення в обліку грошових коштів, одержаних від реалізації отриманого внаслідок шахрайських дій майна; визначення кола осіб, причетних до вчинення шахрайства, та обставин, що сприяли вчиненню кримінального правопорушення [219].

Щодо особи, то тут, як правило, назначається судово-психіатрична експертиза підозрюваного і проводиться вона тоді, коли відносно нього виникає сумнів в його психічній повноцінності. На вирішення цієї експертизи ставиться такий перелік питань:

Чи страждає підозрюваний якими-небудь психічними захворюваннями, якщо страждає, то чи міг він усвідомлювати свої дії, або керувати ними при вчиненні інкримінованого йому діяння?

Чи не знаходився підозрюваний у момент вчинення кримінального

правопорушення в тимчасово хворобливому стані та чи міг він усвідомлювати свої дії чи керувати ними?

Чи не є підозрюваний душевнохворим, якщо так, то чи не потребує він застосування примусових заходів медичного характеру?

Якщо в особи є відхилення психіки, то чи не позбавляють вони здатності усвідомлювати свої дії та керувати ними? [24].

Вказані переліки експертиз і питань до них не є вичерпними.

Підсумовуючи викладене у підрозділі, зазначимо, що, здійснивши аналіз поглядів наведених вище та інших криміналістів, а також спираючись на результати вивчення кримінальних проваджень (Додаток Б) та опитування працівників слідчих підрозділів НП України (Додаток В), можна зробити висновок, що під час проведення досудового розслідування шахрайств, які вчиняються з використанням ЕОТ, повинні призначатися такі експертизи:

експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза), де об'єктом дослідження є ЕОТ, програмні продукти, з використанням яких вчинялося шахрайство;

експертиза телекомунікаційних систем і засобів, де об'єктом дослідження є телекомунікаційні системи й засоби, які використовувались особою з метою спілкування під час вчинення обману чи зловживання довірою потерпілого, а також для функціонування ЕОТ при вчиненні шахрайства;

молекулярно-генетична експертиза, де об'єктом дослідження є кров, сперма, букальний епітелій, слина, піднігтьовий вміст, кістки і зуби, волосся з цибулиною;

дактилоскопічна експертиза, де об'єктом дослідження можуть бути відбитки слідів рук осіб, які були вилучені з ЕОТ, телекомунікаційних систем і засобів, предметів, які були об'єктом шахрайства, документів, які утворювались під час вчинення вказаного кримінального правопорушення;

експертиза матеріалів і засобів звукозапису, де об'єктом дослідження можуть бути: а) записи дій та переговори осіб, причетних до шахрайства, або

відео-, аудіозаписів, вчинених під час купівлі/продажу (передачі/отримання) предмета шахрайства; б) технічні засоби знімання та фіксації інформації;

технічна експертиза документів та експертиза матеріалів документів, де об’єктом є підроблені документи, які використовувались з метою вчинення шахрайства;

експертиза документів бухгалтерського, податкового обліку і звітності, де об’єктом дослідження є документи, що відображають проведення фінансово-кредитних операцій, а також економічної діяльності суб’єкта господарської діяльності, який вчиняє певні шахрайські дії.

Щодо особи, як правило, проводиться судово-психіатрична експертиза підозрюваного.

Висновки до розділу 3

Однією з найбільш важливих слідчих (розшукових) дій під час розслідування шахрайств, учинених з використанням ЕОТ, є обшук, проведення якого забезпечує отримання доказової інформації про подію кримінального правопорушення та осіб, які його вчинили (зазначили 95 % проанкетованих слідчих). Визначено, що особливістю проведення обшуку у досліджуваних кримінальних провадженнях є: а) необхідність у спеціальних знаннях про структуру та роботу ЕОТ, програмного забезпечення, засобів телекомунікації; б) забезпечення безпечного огляду ЕОТ, отримання відповідних паролів з метою подальшого доступу до інформації, яка знаходиться в ЕОТ; в) дотримання відповідних правил виявлення, вилучення та упакування ЕОТ, інших предметів під час обшуку.

Зроблено висновок, що проведення допитів у кримінальних провадженнях про шахрайства, учинені з використанням ЕОТ, вимагає від слідчих обізнаності у спеціальних питаннях щодо процесу побудови сайтів, інших акаунтів, розміщення на них повідомлень і специфіки використання

при цьому відповідного програмного забезпечення та обладнання. Вказане потребує попередньої підготовки до допиту слідчим, що повинно включати: одержання від спеціаліста довідкових даних про місце, час створення сайтів, спосіб і час розміщення на них певної інформації, при цьому доцільно запросити на допит спеціаліста, яким чином і звідки здійснювалось адміністрування сайтом, акаунтом; коли були створені електронні скриньки та як вони використовувались у злочинних цілях.

Зазначено, що під час розслідування шахрайств, учинених з використанням ЕОТ, важливою є участь спеціаліста, допомога якого необхідна для: а) застосування науково-технічних засобів і прийомів задля виявлення, фіксації та вилучення ЕОТ й інших предметів, за допомогою яких здійснювалися шахрайські дії; б) визначення способу та механізму використання ЕОТ під час вчинення шахрайства; в) пошуку слідів і речових доказів, вилучення слідів, зразків та інших об'єктів, які мають відношення до шахрайства, учиненого з використанням ЕОТ, а також у збереженні вилучених ЕОТ та комп'ютерних програм; г) надання довідкових відомостей, консультацій слідчих та інших учасників слідчої (розшукової) дії з приводу застосування спеціальних знань; д) допомоги слідчому щодо правильності викладення виявлених відомостей у протоколі, а також у складанні схем, планів місця розташування й підключення ЕОТ та інших предметів; е) формулювання питань особам, яких будуть допитувати у зв'язку з їх перебуванням на місці кримінального правопорушення.

Водночас у процесі розслідування шахрайств, учинених з використанням ЕОТ, проводяться наступні види експертиз, які забезпечують повне та всебічне розслідування цих кримінальних правопорушень: 1) експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза), де об'єктом дослідження може бути: ЕОТ (системні блоки комп'ютерів, ноутбуки, планшети, айподи, сервери, стільникові телефони тощо та їх комплектуючі); периферійні пристрої, які використовувались під час виходу ЕОТ в Інтернет-мережу (зовнішні модеми,

адаптери комп’ютерних мереж, перемикачі, маршрутизатори, комутатори, стільникові телефони, супутникова телефонія тощо); носії інформації (накопичувачі на жорстких оптичних і лазерних дисках (CD, DVD, Blue-ray), комп’ютерні дискети, оптичні компакт-диски, флеш-картки пам’яті, HDD та SSD бокси тощо); електронні записні книжки, планшети та інші електронні носії текстової або цифрової інформації; 2) експертиза телекомунікаційних систем і засобів, де об’єктами є: телекомунікаційні системи (наприклад, системи мобільних операторів зв’язку, телевізійні системи, радіосистеми тощо); мобільні термінали (наприклад, телефони, смартфони, планшети та інші мобільні пристрої, із встановленим програмним забезпеченням; білінгові системи (наприклад, білінгові системи мобільних операторів, білінгові системи банків, системи державних реєстрів тощо); спеціалізовані технічні пристрої (наприклад, станції активних перешкод, телематичні модулі, пульти керування доступом, програматори активних ключів для автомобілів та іммобілайзерів тощо); Інтернет IP-вузли; доменні імена, вебсторінки, адресація в мережі Інтернет; передавачі радіосигналів; приймачі радіосигналів; вузли комутації; первинні мережі зв’язку; наземні станції супутникового зв’язку; периферійні пристрої, які використовувались під час виходу ЕОТ в Інтернет-мережу (зовнішні модеми, адаптери комп’ютерних мереж, перемикачі, маршрутизатори, комутатори, стільникові телефони, супутникова телефонія тощо); 3) молекулярно-генетична експертиза, де об’єктом дослідження може бути: кров, сперма, букальний епітелій, слина, піднігтьовий вміст, кістки і зуби, волосся з цибулиною; 4) дактилоскопічна експертиза, де об’єктом дослідження можуть бути: а) відбитки слідів рук осіб, які були вилучені з ЕОТ та інших предметів, а також у приміщенні, де здійснювалось використання ЕОТ з метою вчинення шахрайства; б) відбитки слідів рук осіб, які можуть бути причетні до отримання предмета шахрайства (майна); 5) експертиза матеріалів і засобів звукозапису, де об’єктом дослідження можуть бути записи дій та переговори осіб, причетних до вчинення шахрайства, з використанням ЕОТ; 6) технічна експертиза

документів, де об’єктом дослідження можуть бути: документи, що засвідчують особу, подію, освіту, трудовий стаж (паспорт; свідоцтва про народження, одруження і розірвання шлюбу, зміну прізвища, імені, по батькові; трудова книжка та вкладиш до неї; посвідчення водія, службові, військові, ветеранів, інвалідів; дипломи про освіту, присвоєння звання; пенсійна книжка; пенсійні листки; листи тимчасової непрацездатності тощо); проїзні документи (квитки на проїзд залізничним, морським, річковим, повітряним і міським транспортом; документи на перевезення вантажів тощо); документи, що обслуговують грошовий обіг (книжки ощадні, чекові, депозитні; чеки грошові, майнові, розрахункові; бланки фінансування, страхування; акредитиви; марки податкові, митні, акцизні; доручення на видачу коштів, пенсій, майна; сертифікати якості, на право вивезення та ввезення, поліси страхування; ліцензії тощо); білети тиражних і миттєвих лотерей; цінні папери (акції, облігації, казначейські зобов’язання, ощадні сертифікати, приватизаційні папери, векселя тощо); інші документи та цінні папери, передбачені чинним законодавством; слідоутворюючі поверхні засобів письма та інших технічних засобів (друкарських форм, печаток, штампів тощо), за допомогою яких виготовляються документи та їх реквізити на певних матеріальних носіях; зміст документів (текст, підписи, відбитки печаток, штампів тощо); 7) експертиза матеріалів документів, де об’єкт дослідження співпадає з об’єктом технічної експертизи документів, а також інші види експертиз. Щодо особи, як правило, назначається судово-психіатрична експертиза підозрюваного і проводиться вона тоді, коли відносно нього виникає сумнів в його психічній повноцінності.

ВИСНОВКИ

У **висновках** дисертації на підставі узагальнення основних положень та результатів проведеного дослідження проблем розслідування шахрайств, учинених з використанням ЕОТ, сформульовано такі висновки й рекомендації, що відповідають вимогам наукової новизни, а також мають теоретичне і практичне значення:

1. Проблема розслідування шахрайств, учинених з використанням ЕОТ, наразі залишається недостатньо дослідженою, незважаючи на актуальність тематики. Більшість публікацій (Т. А. Пазинич «Криміналістична характеристика шахрайств та основні положення їх розслідування» (2007), О. Л. Мусієнко «Теоретичні засади розслідування шахрайства в сучасних умовах» (2008), А. В. Крижевський «Криміналістична характеристика шахрайств у сфері мобільного зв'язку», С. С. Чернявський «Теоретичні та практичні основи методики розслідування фінансового шахрайства» (2010), Т. В. Охрімчук «Криміналістична характеристика шахрайства з фінансовими ресурсами та основні напрями розслідування» (2011), А. І. Анапольська «Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків» (2011), С. М. Князєв «Розслідування шахрайства, вчиненого способом фінансової піраміди» (2012), С. В. Самойлов «Розслідування шахрайств, учинених із використанням мережі «Інтернет»» (2014)) стосуються лише криміналістичної характеристики шахрайств, учинених з використанням ЕОТ, визначення окремих напрямів проведення слідчих (розшукових) дій під час розслідування вказаних кримінальних правопорушень, а також особливостей огляду комп'ютерної техніки. Вони не охоплюють повного комплексу питань, пов'язаних з розслідуванням шахрайств, учинених з використанням ЕОТ. Зазначене потребує першочергового опрацювання проблемних питань, що виникають, зокрема, під час встановлення місцезнаходження ЕОТ, яка використовувалась з метою вчинення

шахрайства, вилучення, огляду та дослідження ЕОТ і матеріальних, і віртуальних слідів шахрайства.

2. Предмети шахрайства, учиненого з використанням ЕОТ, умовно можна поділити на: а) рухомі та нерухомі речі (майно); б) права на майно. Майно як предмет шахрайства повинно володіти певними фізичними, економічними, юридичними ознаками, де: 1) фізичні ознаки – це предмети, речі, матеріальні предмети зовнішнього світу, які можна вилучити, привласнити, спожити, пошкодити, знищити тощо; 2) економічні ознаки – майно має становити певну матеріальну цінність, мати певну вартість, грошову оцінку (товарно-матеріальні цінності, гроші, валютні цінності й цінні папери (акції, облігації), що є еквівалентом); 3) юридичні ознаки – право на майно належить певному власнику або особі, якій воно на законній підставі ввірене, перебуває у її віданні чи під її охороною, для винного майно є чужим. До речових прав відноситься: право власності, право довічного володіння, а до зобов'язальних – право оренди, зберігання найму. Особливістю предмета шахрайства, вчиненого з використанням ЕОТ, є заволодіння інформацією про власників платіжних банківських карток та їх реквізити. До такої інформації, як правило, належить: а) ім'я та прізвище держателя картки; б) назва/ код структурного підрозділу банку, що випустив картку; в) термін дії картки; г) номер картки.

До найбільш поширених в Україні способів шахрайств, учинених з використанням ЕОТ, належать: 1) заволодіння інформацією *у* власників платіжних карток про їх реквізити та іншу конфіденційну інформацію й подальше заволодіння коштами з банківського рахунку потерпілого; 2) створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих товарів; 3) заволодіння майном шляхом створення та діяльності фіктивних фінансових бірж; 4) заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій; 5) заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину, а також інші способи. Криміналістичне

значення способу кримінального правопорушення полягає в тому, що за ним можна встановити типові сліди, тобто сліди, які залишає безпосередньо злочинець, використовуючи ЕОТ з метою вчинення шахрайства.

3. Слідова картина шахрайств, учинених з використанням ЕОТ, характеризується, як правило, наявністю цифрових слідів, що були створені злочинцем і знайшли своє відображення у вигляді інформації: а) на оперативному запам'ятовуючому пристрої, жорсткому диску, запам'ятовуючому пристрої комп'ютерної техніки, стільникового телефону потерпілого у вигляді слідів активності в Інтернет-мережі залишені при перегляді інтернет-сайтів та у подальшому здійсненні купівлі/продажу предмета шахрайства; б) в електронній поштовій скриньці потерпілого – під час здійснення ним електронної переписки зі злочинцем; в) як профіль у соціальних мережах як потерпілого, так і злочинця; г) внаслідок проведення банківських платежів між потерпілим і злочинцем. Обстановка вчинення шахрайств з використанням ЕОТ засвідчує, що такі злочини вчиняються у віртуальному середовищі, де залишаються лише інформаційні сліди. Місце вчинення таких видів шахрайств і місце події не завжди становлять єдиний комплекс. Типовими місцями таких кримінальних правопорушень є місце проживання злочинця, місце роботи, місця позбавлення волі, а також спеціально вибрані місця, де є доступ до мережі Інтернет через WI-FI (заклади харчування, громадські місця). Непоодинокі випадки використання ЕОТ з метою вчинення шахрайства поза межами нашої держави або у тимчасово окупованих районах Донецької та Луганської областей, Автономної Республіки Крим. Майже завжди шахраї використовують спеціальні програми (VPN-з'єднання та їх аналоги), що захищають конфіденційність IP-адрес, з яких вони виходять в Інтернет-мережу з метою вчинення протиправних дій.

4. Однією з характерних особливостей шахрайства, які вчиняються з використанням ЕОТ, є різноманітність особи злочинця. Вказане кримінальне правопорушення вчиняють особи, які володіють незначними знаннями в

сфері інформаційно-телекомунікаційних технологій, так і особами, які володіють спеціальними знаннями у цій сфері. Специфікою даного виду шахрайства є те, що постраждати від нього може практично кожен. При цьому підкреслено, що вивчення особи злочинця є передумовою процесу висунення слідчих версій і планування розслідування, дає змогу обрати найбільш оптимальні тактичні прийоми проведення слідчих (розшукових) дій, а також окреслити коло осіб, які причетні до вчинення цього кримінального правопорушення.

5. Окреслюючи обставини, які підлягають встановленню під час розслідування шахрайств, учинених з використанням ЕОТ, визначено, що вони є сукупністю обставин, сформованих з норм кримінального і кримінального процесуального права, також необхідно встановити для реалізації завдань кримінального судочинства, з одночасним поєднанням обставин, які безпосередньо не зазначені в КПК України.

6. Виокремлено типові слідчі ситуації початкового стану розслідування досліджуваних кримінальних правопорушень залежно від обсягу та змісту інформації про особу (осіб), яка вчинила кримінальне правопорушення: а) 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; б) встановлено факт шахрайства, учиненого з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї.

З урахуванням вихідної інформації визначено типові слідчі версії під час розслідування шахрайства, учиненого з використанням ЕОТ, зокрема: 1) щодо наявних відомостей про особу; 2) щодо кількості злочинців; 3) щодо механізму вчинення шахрайства та побудови вебсторінки, яку використовували для вчинення кримінального правопорушення; 4) щодо поінформованості злочинця про співучасників шахрайства; 5) щодо кількості вчинених кримінальних правопорушень та їх поширеності; 6) щодо місця

розташування ЕОТ, з якого злочинці вчиняли контакти з потерпілим; 7) щодо мотиву вчинення шахрайства; 8) щодо кількості залучених до злочинної діяльності ЕОТ. У розвиток кожної з вказаних вище версій надалі висуваються окремі версії, що ґрунтуються на конкретних даних, зібраних у кримінальному провадженні, найбільшої уваги серед яких заслуговують окремі версії, що стосуються особи, яка вчинила кримінальне правопорушення.

7. Визначено основні напрями розслідування шахрайств, учинених з використанням ЕОТ. Акцентовано увагу на процесуальних діях, призначення яких надасть можливість встановити IP-адреси ЕОТ, з використанням яких вчинялися шахрайства, безпосереднє місцезнаходження таких ЕОТ, а також встановлення осіб, які брали участь у такому шахрайстві: 1) надання письмових доручень оперативним підрозділам НП України з метою встановлення IP-адрес інтернет-ресурсу (вебсайту), ЕОТ і засобів комунікації, які використовувались з метою вчинення шахрайства, у т.ч з проведенням негласних (слідчих) розшукових дій; 2) здійснення тимчасового доступу до документів інтернет-провайдерів з метою отримання інформації щодо осіб, причетних до створення (власників) інтернет-ресурсу (вебсайту), осіб, які здійснюють їх адміністрування, а також безпосередніх користувачів: а) про реєстрацію доменного імені та хостінгу з якого здійснювалось шахрайство; б) про реєстрацію IP-адреси чи поштової скриньки користувача Інтернет-мережі, причетного до шахрайства, вчиненого з використанням ЕОТ; в) про адміністрування інтернет-форуму або чату, через який здійснював спілкування потерпілий під час вчинення шахрайських дій щодо нього; 3) зняття інформації з електронних інформаційних систем щодо поштових скриньок, які використовувались для спілкування під час вчинення шахрайства; 4) тимчасовий доступ до речей та документів інтернет-провайдерів, IP-адреси яких використовували під час вчинення шахрайства; 5) тимчасовий доступ до операторів телефонного зв’язку – щодо отримання переписки й трафіку дзвінків особи, яка спілкувалась з потерпілим під час

вчинення шахрайства; 6) установлення місцезнаходження радіоелектронного засобу, а саме мобільного телефону, який використовувався під час вчинення шахрайства, з метою локалізації місцезнаходження такого телефону і встановлення його користувача; 7) тимчасовий доступ до інформації, яка була відзнята камерами відеоспостереження чи відеореєстраторами за місцем використання IP-адрес, з яких вчинялось шахрайство з використанням ЕОТ, і здійснення подальшого огляду таких записів з метою встановлення осіб у приміщеннях чи інших місцях, з яких виходив у мережу Інтернет з використанням ЕОТ за певною IP-адресою; 8) проведення обшуків у приміщеннях за місцем встановлення ЕОТ і засобів комунікації, IP-адреси яких використовувались для вчинення шахрайських дій з використанням ЕОТ; 9) надання доручення оперативному підрозділу НП України в порядку ст. 40 КПК України на проведення комплексу інших НСРД, спрямованих на встановлення місцезнаходження ЕОТ, яка використовувалась під час шахрайства, здійснення організаційних заходів з метою персоналізації відомостей про користувачів, а також пошуку інформації в інформаційно-пошукових системах НП України.

8. Особливості тактики обшуку місцезнаходження ЕОТ, а також подальший огляд такої техніки під час розслідування шахрайств визначаються змістом їхніх завдань: 1) виявлення ознак, які свідчать, що ЕОТ використовувалась з метою вчинення шахрайства; 2) визначення точного місця (приміщення) та часу використання ЕОТ з метою вчинення шахрайства для подальшого виявлення криміналістично значущої інформації, встановлення цифрових слідів такої протиправної діяльності; 3) встановлення ознак і факторів, які свідчать, що кримінальне правопорушення вчинено певною ЕОТ та особою, а також виявлення матеріальних і віртуальних слідів, які вони залишили; 4) підтвердження способу використання ЕОТ з метою вчинення шахрайства; 5) виявлення додаткових предметів, що свідчать про використання ЕОТ для вчинення шахрайства; 6) встановлення додаткових можливостей виявлення доказової

інформації. Обшук передбачає обов'язкове залучення спеціаліста для його проведення, організацію проведення додаткових інструктажів для учасників цієї слідчої (розшукової) дії, вжиття заходів щодо забезпечення безпеки виявлення, вилучення, упакування, перевезення та зберігання вилучених ЕОТ й інших предметів під час цієї слідчої (розшукової) дії.

Зважаючи на те, що певна кількість віртуальної інформації зберігається на ЕОТ, виникає необхідність у безпечному вилученні як самої ЕОТ, так і інформації, яка у ній міститься і, відповідно, їх огляду. У зв'язку з чим визначено: а) організаційні особливості підготовки до огляду ЕОТ та наявної в ньому інформації; б) розкрито порядок початкового етапу огляду; в) проведення безпосереднього огляду фізичних носіїв ЕОТ та наявної на них інформації (внутрішні та зовнішні фізичні носії пам'яті, оперативні запам'ятовуючі пристрої ЕОТ, периферійних пристроїв і засобів зв'язку); г) особливості складання протоколу за результатами такого огляду.

9. За результатами узагальнення практичного досвіду встановлено, що під час допиту осіб, які використовували ЕОТ з метою вчинення шахрайства, найчастіше слідчі застосовують такі тактичні прийоми: пред'явлення особі, яку допитують, речових доказів та інших матеріалів провадження, що свідчать про користування нею певною ЕОТ, створення та подальше адміністрування вебпорталом (сайтом), здійснення електронної переписки з потерпілим (або здійснення телефонних переговорів), або спростовують її алібі (95,7 %); оголошення показань інших підозрюваних, потерпілих, свідків (60,1 %); використання суперечностей у самих показаннях допитуваного або з іншими доказами (25,0 %); максимальна деталізація показань з метою виявлення суперечностей (16,3 %); надання пропозиції повторного викладення показань про подію загалом або окремі її обставини (13,7 %); вияв розуміння становища, в якому опинилася особа, яку допитують (12,0 %); переконання в необхідності повідомлення правдивих відомостей (4,7 %); спонукання до каяття шляхом формування внутрішнього протесту проти вчинених дій (2,3 %); інше (0,3 %).

10. Особливість залучення спеціаліста до проведення обшуку місця зберігання ЕОТ полягає в необхідності: а) роз'яснення учасникам його проведення заходів безпеки при поводженні з ЕОТ, а також іншими засобами й предметами, які оглядаються та вилучаються; б) приведення ЕОТ та інших пристроїв у безпечний стан, встановлення наявних паролів доступу як безпосередньо до ЕОТ, так і наявних у ньому програм, а також паролів до вебсторінок, сайтів, пошти тощо, що дозволяє у подальшому їх оглянути та дослідити експертові; в) надання слідчому допомоги в огляді та фіксації інформації працюючої ЕОТ, зокрема з екрану монітору; г) надання допомоги слідчому у вилученні, упакуванні, опечатуванні та перевезенні ЕОТ, інших носіїв інформації (накопичувачі пам'яті, мікропроцесори, оперативна пам'ять тощо) та інших предметів для подальшого їх дослідження в лабораторних умовах; д) забезпечення безпечного зберігання ЕОТ та інших вилучених предметів; е) надання допомоги слідчому щодо правильності викладення виявлених відомостей у протоколі, а також у складанні схем способу під'єднання периферійних засобів до ЕОТ; є) формулювання питань особам, яких опитують та котрі перебувають на місці виявлення ЕОТ, з метою встановлення паролів доступу як безпосередньо до ЕОТ, так і наявних у ньому програм, а також паролів до вебсторінок, сайтів, електронної пошти тощо.

11. Систематизовано види судових експертиз, які необхідно призначати при розслідуванні шахрайств, учинених з використанням ЕОТ, зокрема щодо: а) ЕОТ і периферійних пристроїв – комп'ютерно-технічна експертиза (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення) стосовно виявленої (вилученої) інформації; молекулярно-генетична експертиза стосовно вилучених біологічних об'єктів; дактилоскопічна експертиза стосовно вилучених слідів рук з ЕОТ); б) телекомунікаційних засобів і систем – експертиза телекомунікаційних систем та засобів; молекулярно-генетична експертиза стосовно вилучених біологічних об'єктів; дактилоскопічна експертиза стосовно вилучених слідів

рук з телекомунікаційних засобів і систем; в) документів – криміналістична почеркознавча експертиза; технічна експертиза документів; дактилоскопічна експертиза вилучених слідів рук з документів; г) майна, яке було предметом посягання – криміналістична експертиза матеріалів, речовин і виробів; трасологічна експертиза; молекулярно-генетична експертиза стосовно вилучених біологічних об'єктів; дактилоскопічна експертиза стосовно вилучених слідів рук з різних предметів. Щодо особи: а) судово-наркологічна експертиза; б) судово-психіатрична експертиза; в) комплексна судова психіатрична та наркологічна експертиза.

Сформульовано перелік питань, які ставляться перед експертом під час проведення зазначених вище криміналістичних експертиз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 11 лучших бесплатных VPN-сервисов для компьютеров и смартфонов. URL: https://lifehacker.ru/free-vpn/

2. Cherniavskyi S., Ortynskyy V., Rohatiuk I., Udalova L., Sirant M. Investigation of Crimes of an International Character. *Gournal of Legal, Etnical and Regulatory Issues* (Print ISSN: 1544-0036; Online ISSN:1544-0044). *Journal of Legal, Ethical and Regulatory Issues*. 2019. Vol. 22. Iss. 5. P. 1–15.

3. Kryshevych O., Andrushchenko I., Striltsiv O., Pyvovar Y., Rivchachenko O. Modern methods of computer-related fraud: legal characteristics and qualification. *Cuestiones Políticas*. Vol. 39. №º68 (Enero-Junio) 2021. P. 844–865.

4. Padgett S. Profiling the Fraudster: Removing the Mask to Prevent and Detect Fraud. 2014. 272 p. Doi: 10.1002/9781118929773

5. Susan H. Nycum. The Criminal Law Aspects of Computer Abuse: Applicability ofthe State Penal Laws to Computer Abuse (Menlo Park, California, Stanford Research Institute, 1976). *Ulrich Sieber, Computerkriminalität und Strafrecht (Cologne, Karl Heymanns Verlag, 1977).* URL: http://www.worldcat.org/title/criminal-law-aspects-of-computer-abuse-applicability-of-the-state-penal-laws-to-computerabuse/oclc/654145221/editions?referer=di&editionsView=true

6. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. Сєвєродонецьк, 2017. № 1 (77). С. 168–174.

7. Авдєєва Г. К. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за заг. ред. В. Ю. Шепітька, В. А. Журавля. Харків: Вид. агенція «Апостіль», 2017. 238 с.

8. 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.

9. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження). Монографія. Київ: Атіка, 2007. 304 с.

10. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: дис. ... канд. юрид. наук: 12.00.08 «Кримінальний процес, криміналістика, судова експертиза». Київ, 2003. 246 с.

11. Алауханов Е. Криминология: учебник. Алматы, 2008. 429 с.

12. Александров О. О., Дудоров В. А., Клименко В. А. та ін. Кримінальне право України. Особлива частина: підручник / за ред. М. І. Мельника, В. А. Клименка. 3-тє вид., переробл. та допов. Київ: Атіка, 2009. 744 с.

13. Аналоги Hideman VPN. URL: https://ruprogi.ru/software/hideman

14. Анапольська А. І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Харків, 2011. 18 с.

15. Анапольська А. І. Тактичні особливості допиту підозрюваного по справах про розкрадання грошових коштів, вчинених у сфері функціонування електронних розрахунків. *Форум права.* 2009. № 3. С. 19–24.

16. Антощак А. Р. Обставини, що підлягають встановленню під час розслідування привласнення, розтрати або заволодіння майном, шляхом зловживання службовою особою своїм службовим становищем. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2016. Вип. 38 (2). С. 95–98.

17. Атаманов Р. С. Основы методики расследования мошенничества в сети Интернет: автореф. дис. … канд. юрид. наук: 12.00.09. «Криминальный процесс, криминалистика, судебная экспертиза». Москва, 2012. 28 с.

18. Ахтирська Н. М., Томас Ж. Ю. Актуальні питання розслідування злочинів проти власності: навч. посіб. К.: ВПЦ «Київський університет», 2018. 246 с.

19. Барабаш Т. М. Предмет доказування у кримінальних справах про ухилення від сплати податків, зборів, інших обов'язкових платежів: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Київ, 2002. 210 с.

20. Батюк О. В., Благута Р. І., Гумін О. М. та ін. Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ: навч. посіб. / за заг. ред. Є. В. Пряхіна. Львів: ЛьвДУВС, 2011. 324 с.

21. Баулін Ю. В. Звільнення від кримінальної відповідальності: монографія. Київ: Атіка, 2004. 296 с.

22. Баулін Ю. В., Борисов В. І., Кривоченко Л. М. Кримінальне право України. Загальна частина. 3-тє вид., переробл. і допов. Київ: Юрінком Інтер, 2007. 456 с.

23. Бахін В. П., Зав'ялов С. М. Актуальні проблеми способу вчинення злочинів за умов істотної зміни характеру злочинної діяльності. *Наук. вісник Нац. акад. внутр. справ України.* 2000. № 2. С. 178–182.

24. Бедь В. В. Юридична психологія: навч. посіб. 2-ге вид., доп. і переробл. Київ, МАУП. 436 с.

25. Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы (от теории к практике). Москва, 1988. 304 с.

26. Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы. Общая и частная теории. Москва, Юрид. лит., 1987. 272 с.

27. Берназ В. Д. К вопросу о понятии обстановки совершения краж социалистического имущества на морском транспорте. *Криминалистика и судебная экспертиза.* Вып. 31. Киев, Вища шк., 1985. С. 44–47.

28. Бишевець О. В. Використання спеціальних знань у доказуванні в кримінальних провадженнях. *Вісник кримінального судочинства.* 2015. № 2. С. 187–193.

29. Бишевець О. В., Погорецький М. А., Сергеева Д. Б. та ін. Розслідування окремих видів злочинів: навч. посіб. / за ред. М. А. Погорецького та Д. Б. Сергєєвої. Київ: Алерта, 2015. 536 с.

30. Бідняк Г. С. Використання спеціальних знань при розслідуванні шахрайств: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Дніпро, 2018. 218 с

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

32. Бідняк Г. С. Участь спеціаліста у проведенні огляду документів під час розслідування шахрайств. *Криміналістичний вісник.* 2016. № 1. С. 162–166.

33. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Київ, 2008. 20 с.

34. Борисова Л. В. Транснаціональні комп’ютерні злочини як об’єкт криміналістичного дослідження: дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Київ, 2007. 217 с.

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

36. Бурчак Ф. Г., Фесенко Е. Ф. Уголовное право Украинской ССР на современном этапе. Часть Общая: монограф. Киев: Наук. думка, 1985. 448 с.

37. Буряк В. Ю., Геваза Ю. І., Замошець О. П. Експертиза наркотичних речовин: навч. посіб. Київ: Київ. нац. торг.-екон. ун-т, 2004. 266 с.

38. Вакуленко О. В., Стрільців О. М., Тарасенко О. С. та ін. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рек. Київ: Нац. акад. внутр. справ, 2016. 56 с.

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

40. Васильєв В. В. Правове регулювання відшкодування шкоди, завданої злочином: автореф. дис. … канд. юрид. наук: 12.00.03. Цивільне право і цивільний процес; сімейне право; міжнародне приватне право. Харків, 2015. 20 с.

41. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голов. ред. В. Т. Бусел. Київ, Ірпінь : ВТФ «Перун», 2005. 1728 с.

42. Великий тлумачний словник сучасної української мови: (з дод., допов. та CD) / Уклад. і голов. ред. В. Т. Бусел. Київ, Ірпінь: ВТФ «Перун», 2009. 1736 с.

43. Веліканов С. В. До поняття електронного сліду в криміналістиці. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення:* матеріали постійно діючого наук.-практ. семінару (Харків, 27 листоп. 2015 р. Харків: Право, 2015. Вип. 7. С. 241–244.

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

45. Весельський В. К., Пясковський В. В. Торгівля людьми в Україні (проблеми розслідування): навч. посіб. Київ: КНТ, 2007. 268 с.

46. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. рек. / М. В. Гуцалюк, В. Д. Гавловський,

В. Г. Хахановський та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с

47. Виноградова М. М. Спорные вопросы определения пределов компетенции судебных экспертов-экономистов. *Теорія та практика судової експертизи і криміналістики:* зб. наук. праць. Вип. 10. Харків: Право, 2010. С. 540–547.

48. Вирок Кіровоградського районного суду Кіровоградської області від 16 берез. 2020 р. Справа № 390/1749/17. URL: https://reyestr.court.gov.ua/Review/88333314

49. Вирок Корольовського районного суду м. Житомира від 22 трав. 2020 р. Справа № 296/2054/17. URL: https://reyestr.court.gov.ua/Review/89462584

50. Вирок Приморського районного суду м. Одеси від 15 верес. 2016 р. Справа № 63418296. URL: http://www.reyestr.court.gov.ua/Review/63418296

51. Волкотруб С. Г., Омельчук О. М., Ярін В. М. та ін. Кримінальне право України: навч. посіб.; за ред. О. М. Омельчука. Київ: Наук. думка; Прецедент, 2004. 297 с.

52. Волобуєв А. Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки. *Вісник Луганського інституту внутрішніх справ МВС України*. Вип. 2. Луганськ. 1998. 376 с.

53. Воробйова К. В. Криміналістична характеристика шахрайств, що вчиняються у сферах використання електронних технологій. *Від громадянського суспільства – до правової держави:* тези VIII Міжнар. наук. Internet-конф. студентів та молодих вчених. Харків: Харк. нац. ун-т ім. В. Н. Каразіна, 2013. С. 96–99.

54. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі

розслідування: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2008. 216 с.

55. 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.

56. Головкін С. В., Іщенко А. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : монографія. МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. 160 с.

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

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

59. Гора І. В., Іщенко А. В., Колесник В. А. Криміналістика: навч. посіб. 4-те вид., випр. та доповн. Київ: ПАЛИВОДА А. В., 2007. 236 с.

60. Горелик И. И. Мотив и цель преступления. Уголовное право БССР. Часть общая: в 2 т. Минск: Высш. шк., 1978. Т. 1. 334 с.

61. Грамович Г. И. Тактика использования специальных знаний в раскрытии и расследовании преступлений: учеб. пособ. Минск: МВШ МВД СССР, 1987. 66 с

62. Гринчак О. Що варто знати про кіберзлочинців в Україні. 2018 URL: https://www.radiosvoboda.org/a/details/29031166.html

63. Гросс Г. Руководство для судебных следователей как система криминалистики: перепеч. с нем. 4 доп. изд. / Л. Дудкина и Б. Зиллера. СПб., 1908. XXVII, 1040 с.

64. Грошевой Ю. М. Освобождение от уголовной ответственности в стадии судебного разбирательства: учеб. пособ. Харьков: Вища шк.: Изд. при Харьк. ун-те, 1979. 144 с.

65. Гусаченко Є. О. Слідчий експеримент: використання спеціальних знань та умови їх нормативного застосування. *Науковий вісник Херсонського державного університету.* 2015. Вип. 1. С. 98–103.

66. Давиденко В. С. Спеціальні знання в розслідуванні економічних злочинів. *Юридичний часопис Нац. акад. внутр. справ.* 2016. № 2 (12). С. 178–188.

67. Дехтярьов Є. В. Особливості тактики допиту особи, яка підозрюється у вчиненні шахрайства в сфері виконання господарсько-договірних зобов'язань. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2011. № 3. С. 286–292.

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

69. Дрозд В. Г., Абламский С. Е., Романюк В. В., Симонович Д. В. Актуальные вопросы защиты прав лица, в отношении которого предполагается применение принудительных мер медицинского характера или решается вопрос об их применении. *Журнал Georgian Medical News.* 2019. № 5 (290). С. 150–157.

70. Дрозд В. Г., Руснак Ю. И., Олишевский А. В., Гапотий В. Д. Получение образцов для экспертизы в уголовном производстве: проблемы нормативной регламентации и правоотношения. *Журнал Georgian Medical News* № 7-8. 2019. С. 129–133.

71. Дудніков А. Л. Спосіб злочину у сфері економічної діяльності як системоутворюючий елемент криміналістичної характеристики. *Теорія та практика судової експертизи і криміналістки.* 2017. Вип. 17. С. 39–47.

72. Дудоров О. О. Про конституційність інституту звільнення від кримінальної відповідальності. *Вісник Національної академії прокуратури України.* 2009. № 1. С. 40–48.

73. Експертна служба МВС України. Державний науково-дослідний експертно-криміналістичний центр. *Офіційний вебсайт.* URL: https://dndekc.mvs.gov.ua

74. Ендольцева А. В. Институт освобождения от уголовной ответственности: проблемы и пути их решения: монографія. Москва: ЮНИТИ-ДАНА; Закон и право, 2004. 231 с.

75. Ермолович В. Ф. Криминалистическая характеристика преступлений. Минск: Амалфея, 2001. 304 с.

76. Житомирський науково-дослідний експертно-криміналістичний центр МВС України. *Офіційний вебсайт.* URL: https://www.ndekc.zhitomir.ua/tekhnichna-ekspertiza-dokumentiv

77. Журавель В. А. Обставини, що підлягають з'ясуванню, у структурі криміналістичної методики. *Теорія та практика судової експертизи і криміналістики*. 2010. Вип. 10. С. 12–20.

78. Журавель В. А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія і практика судової експертизи і криміналістики.* 2008. Вип. 8. С. 102–108.

79. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2008. 230 с.

80. Заєць І. В. Шахрайство в господарському процесі українських підприємств. *Вісник ЖДТУ.* Серія : Економічні науки. 2010. № . Ч. 1. С. 80–82.

81. Закатов А. А., Оропай Ю. Н. Использование научно-технических средств и специальных знаний в расследовании преступлений. Киев: РИО МВД УССР, 1980. 104 с.

82. Замошець О. П. Актуальні питання експертизи наркотиків. *Ліки України.* 2004. № 9 (додаток). С. 85–86.

83. Запорощенко Н. А. Розслідування організації або утримання місць для незаконного вживання, виробництва чи виготовлення наркотичних

засобів, психотропних речовин або їх аналогів: дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2012. 281 с.

84. Затенацький Д. В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації): автореф. дис. ... канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза». Харків, 2008. 20 с.

85. Затенацький Д. В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації): монографія / за ред. В. Ю. Шепітька. Харків: Право, 2010. 160 с.

86. Зачек О. І., Захарова О. В., Навроцька В. В., Федчак І. А. Особливості розкриття та розслідування кіберзлочинів: метод. рек. Львів: Львів. держ. ун-т внутр. справ, 2010. 92 с.

87. Зуйков Г. Г. Общие вопросы использования специальных познаний в процессе предварительного расследования. *Криминалистическая экспертиза*. Москва: НИиРИО ВШ МООП РСФСР, 1966. Вып. 1. С. 113–125.

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

89. Інструкції про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 8 січ. 1998 р. № 53/5. *Офіційний вісник України.* № 98. С. 134. Ст. 3591.

90. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: наказ Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5.
URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text

91. Калініна І. В. Ситуаційна обумовленість розслідування господарських злочинів, пов'язаних із підробленням документів. *Ученые записки Таврического национального университета им. В. И. Вернадского*. 2013. Том 26 (65). С. 212–217.

92. Кальман О. Г. Злочинність у сфері економіки України: теоретичні та прикладні проблеми попередження: дис. … доктора юрид. наук: 12.00.08. «Кримінальне право та кримінологія; кримінально-виконавче право». Харків, 2004. 430 с.

93. Капустник Н. Г Оперативний пошук первинної оперативно-розшукової інформації підрозділами кримінальної поліції: зміст поняття. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2019. № 1 (85). С. 243–250.

94. Капустник Н. Г. Наукова розробленість проблеми оперативно-розшукової протидії шахрайству, що вчиняється організованою злочинністю. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. Серія : Право. 2018. № 6. С. 96–100.

95. Керівництво з розслідування злочинів: наук.-практ. посіб. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітька. Харків: Одіссей, 2009. 960 с.

96. Київський науково-дослідний інститут судових експертиз. *Офіційний вебсайт.* URL: https://kndise.gov.ua/activity/expertise-view/c-telekomunikacijna.

97. Кириленко Н. Ю. Методика розслідування шахрайства у сфері побутових відносин: дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Одеса, 2013. 236 с.

98. Кіберполіція припинила діяльність фіктивної фінансової онлайн-біржі. URL: https://www.epravda.com.ua/news/2018/12/11/643459/

99. Кіберполіція припинила діяльність шахрайського call-центру зі щотижневим обігом у 3 мільйони гривень. URL:

https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-shaxrajskogo-call-czentru-zi-shhotyzhnevym-obigom-u--miljony-gryven-6263.

100. Кікінчук В. В. Типові слідчі ситуації початкового етапу розслідування викрадень бюджетних коштів в агропромисловому комплексі. *Право і безпека.* 2013. № 2 (49). С. 131–135.

101. Клименко Н. І. Зміни в правовому регулюванні судово-експертної діяльності. *Криміналістичний вісник*. 2005. № 1. С. 56–60.

102. Князєв С. М. Розслідування шахрайства, вчиненого способом фінансової піраміди: автореф. дис. ... канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Ірпінь, 2012. 19 с.

103. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров’я журналіста. *Вісник Нац. акад. правових наук України.* 2017. № 1 (88). С. 182–191.

104. Ковальчук О. В. Методика розслідування шахрайства, пов’язаного з діяльністю кредитної спілки: дис. ... канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Львів, 2020. 236 с.

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

106. Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений : учеб. пособ. Харьков: Юрид. ин-т, 1985. 93 с.

107. Коментар до ст. 190 Кримінального кодексу України. URL: http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/187.php

108. Комп’ютерно-технічна експертиза. *Центр експертиз. Офіційний вебсайт.* URL: https://expertise.kiev.ua/uk/kompyuterno-texnichna-ekspertiza/

109. Конвенція про кіберзлочинність від 23 листоп. 2001 р. (ратифікована Україною із застереженнями і заявами від 7 верес. 2005 р.). URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575.

110. Коновалова В. Е. Версия: концепция и функции в судопроизводстве. Харків: Консум, 2000. 176 с.

111. Коновалова В. Е., Шепитько В. Ю. Криминалистическая тактика: теории и тенденции: учеб. пособ. Харьков: Гриф, 1997. 256 с.

112. Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: zakon.rada.gov.ua/go/254к/96-вр.

113. Користін О. Є., Бутузов В. М., Василевич В. В. та ін. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. Київ: Видавничий дім «Скіф», 2012. 728 с.

114. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Харків, 2017. 20 с.

115. Косміна Н. М. Використання спеціальних знань при розслідуванні злочинів, пов’язаних з незаконним обігом наркотиків: автореф. дис. … канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза». Харків, 2010. 19 с.

116. Кравченко О. В. Шахрайство *як* складова криміногенної ситуації *в* Україні*:* досвід психологічного дослідження. *Право і Безпека.* 2005. Т. 4. № 2. С. 181–185.

117. Крижевський А. В. Криміналістична характеристика шахрайств у сфері мобільного зв'язку: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2012. 20 с.

118. Криминалистика: учеб. для вузов / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская; под ред. Р. С. Белкина. Москва: Норма–Инфра, 2001. 990 с.

119. Криминалистика: информационные технологии доказывания: учеб. для вузов / под ред. В. Я. Колдина. Москва: Зерцало-М, 2007. 752 с.

120. Криміналістика : підруч. для студ. юрид. спец. вищ. закл. освіти / за ред. В. Ю. Шепітька. 2-ге вид. Київ: Ін Юре, 2004. 728 с.

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

122. Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко, О. О. Алєксєєв та ін. Київ: «Центр учбової літератури», 2015. 544 с.

123. Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і допов. Харків: Право, 2008. 464 с.

124. Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітька. 5-е вид., перероб. і доп. Харків: Право, 2011. 464 с.

125. Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітька. 5-те вид., перероб. та допов. Київ : Ін Юре, 2016. 632 с.

126. Криміналістика: підручник / Нац. акад. внутр. справ. URL: https://pidru4niki.com/2015060965382/pravo/rozsliduvannya_shahraystva

127. Криміналістичне дослідження наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів: метод. рек. / Н. О. Заєць, Р. М. Дем'янчук, І. М. Оленич, Г. В. Лінючев. Київ: ДНДЕКЦ МВС України, 2007. 45 с.

128. Кримінальне право України: Особлива частина: підручник / М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.; за ред. проф. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. 2-е вид., перероб. і доп. Київ: Юрінком Інтер, 2005. 544 с.

129. Кримінальне право України. Загальна частина: практикум: навч. посіб. / І. П. Козаченко, В. К. Матвійчук, О. М. Костенко; за заг. ред. В. К. Матвійчука. Київ: КНТ, 2006. 437 с.

130. Кримінальне право України: Особлива частина: підручник / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін.; за ред. В. В. Сташиса, В. Я. Тація. 4-те вид, переробл. і допов. Харків: Право, 2010. 608 с.

131. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

132. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-V1. *Офіційний вісник України.* 2012. № 37. Ст. 1370.

133. Кримінально-правова кваліфікація та особливості розслідування шахрайства. URL: https://megapredmet.ru/2-12533.html

134. Кримінологічна віктимологія: навч. посіб. / Моісеєв Є. М., Джужа О. М., Василевич В. В. та ін. Київ: Атіка, 2006. 352 с.

135. Кришевич О. В. Кримінально-правова характеристика предмета шахрайства. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2011. № 24. С. 183–191.

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

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

138. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами: автореф. дис. … канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза». Харків, 2002. 20 с.

139. Курята Л. Л. Криміналістичні засади розслідування шахрайства. *Підприємництво, господарство і право.* 2018. № 5. С. 272–275.

140. Літвінчук І. С. Методика розслідування злочинів, пов'язаних із умисним випуском на ринок України небезпечної продукції: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Львів, 2018. 239 с.

141. Лога В. М. Розслідування завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності: дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2012. 220 с.

142. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів: монографія. Київ: НАВСУ, 2005. 360 с.

143. Ляш А. О., Стахівський С. М. Докази і доказування у кримінальному судочинстві: навч. посіб. / за ред. Ю. М. Грошевого. Київ: Університет «Україна», Істина, 2006. 185 с.

144. Марчак В. Я. Консультації та роз'яснення спеціаліста як новела в кримінальному процесуальному законодавстві України. *Митна справа.* 2013. № 2 (86). Ч. 2. Кн. 1. С. 100–105.

145. Матусовський Г. А. Ситуаційний підхід до розслідування злочинів. Криміналістика. Криміналістична тактика та методика: підруч. для вузів / за ред. В. Ю. Шепітька. Харків: Право, 1998. 376 с.

146. МВС України. Офіц. Веб-сайт. URL : https://mvs.gov.ua/ua/news/37913_U_2020_roci_do_kiberpolicii_nadiyshlo_ponad_30_tisyach_zvernen_shchodo_shahraystva_v_Interneti.htm

147. Мединська Л. В. Використання спеціальних знань у кримінальному провадженні України. *Прикарпатський юридичний вісник.* 2014. Вип. 2 (5). С. 278–286.

148. Мельник О. М. Використання електронно-обчислювальної техніки при вчиненні шахрайства. *Вісник інституту економіко-правових досліджень НАН України*. 2011. № 1. С. 57–62.

149. Миколенко О. М. Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів),

систем та комп'ютерних мереж і мереж електрозв'язку. *Кібербезпека в Україні: правові та організаційні питання*: матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовт. 2016 р.). Одеса: ОДУВС, 2016. С. 155–157.

150. Митричев С. П. Методика расследования отдельных видов преступлений. *Криминалистика и судебная экспертиза*. Київ, 1973. Вып. 10. С. 13–28.

151. Михеєнко М. М. Проблеми розвитку кримінального процесу в Україні. Київ: Юрінком Інтер, 1999. 240 с.

152. Моїсеєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів. *Правові основи захисту комп'ютерної інформації від протиправних посягань*: матеріали міжвузівської наук.-практ. конф. (Донецьк, 22 груд. 2000 р.). Донецьк. ін-т внутр. справ, 2001. С. 81–85.

153. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2005. 20 с.

154. Мудряк Т. О. Криміналістичні проблеми розслідування шахрайства з фінансовими ресурсами та шляхи їх вирішення. *Порівняльно-аналітичне право.* 2014. № 1. С. 279–281.

155. Мультимедійний навчальний посібник «Кримінальний процес» / Нац. акад. внутр. справ. URL. https://arm.naiau.kiev.ua/books/public_html/lections/lection10_1.html

156. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах: автореф. дис... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Харків, 2007. 19 с.

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

158. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304–307.

159. Найпопулярніші способи шахрайства в електронній комерції. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-samye-populyarnye-sposoby-moshennichestva-v-elektronnoj-kommercii

160. Науково-дослідний центр судової експертизи з питань інтелектуальної власності Міністерства юстиції України. *Офіційний вебсайт Міністерства юстиції України.* URL: https://intelect.org.ua/activity/expert-activity/telecom/

161. Національна поліція ліквідувала діяльність злочинної групи, яка організувала масштабні шахрайські фінансові біржі. URL : https://slavdelo.dn.ua/2018/12/14/natsionalna-politsiya-likviduvala-diyalnist-zlochinnoyi-grupi-yaka-organizuvala-masshtabni-shahrajski-finansovi-birzhi/

162. Никифорчук В. Д. Характеристика особи кіберзлочинця. *Правові реформи в Україні.* 2013. Ч. 1. С. 181–181.

163. Нор В. Т. Проблеми теорії і практики судових доказів. Львів, 1978. 112 с.

164. Омельяненко М. Особенности криминалистической характеристики Интернет-мошенничества URL: http://kpk.org.ua/2007/12/18/osobennosti-kriminalisticheskojj.html

165. Особливості розслідування окремих видів злочинів: мультимедійний навч. посіб. / Нац. акад. внутр. справ. URL: https://arm.naiau.kiev.ua/books/orovz/lections/lection5.html

166. Охрімчук Т. В. Криміналістична характеристика шахрайства з фінансовими ресурсами та основні напрями розслідування: автореф. дис. ... канд. юрид. наук: спец. 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2011. 16 с.

167. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: автореф. дис. ... канд. юрид. наук:

12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2007. 20 с.

168. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: дис... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2006. 215 с.

169. 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. «Кримінальний процес та криміналістика; судова експертиза». Київ, 2005. 18 с.

170. Панов М. І., Шепітько В. Ю., Коновалова В. О. та ін. Настільна книга слідчого: наук.-практ. видання для слідчих і дізнавачів. Київ: Видавничий Дім «Ін Юре», 2011. 728 с.

171. Панов М. І., Шепітько В. Ю., Коновалова В. О. та ін. Настільна книга слідчого: наук.-практ. видання для слідчих і дізнавачів. К.: Ін Юре, 2003. 720 с.

172. Патик А. А. Взаємодія слідчих та оперативно-розшукових підрозділів при розкритті та розслідуванні майнових злочинів: автореф. дис. ... канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». К., 2011. 17 с.

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

174. Положення про Експертну службу Міністерства внутрішніх справ України: наказ Міністерства внутрішніх справ України від 3 листоп. 2015 р. № 1343. *Офіційний вісник України*. 2015. № 92. С. 342. Ст. 3149.

175. Попов К. Л. Жертва шахрайства: віктимологічне дослідження: автореф. дис. ... канд. юрид. наук: 12.00.08. «Кримінальне право та кримінологія; кримінально-виконавче право». Київ, 2007. 20 с.

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

177. Порубов Н. И. Научные основы допроса на предварительном следствии. 3-е изд., перераб. Минск: Вышэйш. шк., 1978. 175 с.

178. Порядок проведення судово-психіатричної експертизи : затв. наказом Міністерства охорони здоров'я України від 08 жовтня 2001 р. № 397. *Офіційний вісник України*. 2002. № 10. С. 275. Ст. 493. 22 берез.

179. Пошук Інтернет шахраїв. URL: http://private-detective.org.ua/poshuk-internet-shaxra%D1%97v/

180. Про боротьбу з тероризмом: Закон України від 20 берез. 2003 р. № 638-IV. URL: http://zakon.rada.gov.ua/laws/show/638-15.

181. Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події: наказ Міністерства внутрішніх справ України від 3 листоп. 2015 р. № 1339. *Офіційний вісник України.* 2015. № 92. С. 337. Ст. 3148. URL: http://zakon0.rada.gov.ua/laws/show/z1392-15

182. Про судову експертизу: Закон України від 25 лют. 1994 р. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=4038-12

183. Про судову експертизу в кримінальних і цивільних справах: Постанова Пленум Верховного Суду України від 30 трав. 1997 р. № 8 URL: http://zakon3.rada.gov.ua/laws/show/v0008700-97

184. Про судову практику у справах про злочини проти власності: постанова Пленуму Верховного Суду України від 6 листоп. 2009 р. № 10. URL: https://zakon.rada.gov.ua/laws/show/v0010700-09#Text

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

186. Пряхін Є. В. Слідча тактика: навч. посіб. Львів: ЛьвДУВС, 2011. 116 с.

187. Рівчаченко О. А. Розслідування незаконних дій з обладнанням для виготовлення наркотичних засобів, психотропних речовин та їх аналогів: дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2016. 260 с.

188. Рогатюк І. В. Кримінальна процесуальна діяльність прокурора: сутність та зміст. *Науковий вісник Херсонського державного університету*. Серія «Юридичні науки». 2017. Вип. 2. Т. 4. С. 80–83.

189. Розробка спеціальних програмних засобів для проведення судових експертиз комп'ютерних мереж / О. Башкатов, Г. Дружинін та ін. Донецьк : ДНДІСЕ, 2010. 179 с.

190. Романенко Т. В. Алгоритм дій слідчого з розслідування шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні питання криміналістики* : матеріали Всеукр. наук.-практ. конф. (Київ, 20 груд. 2019 р.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ: Нац. акад. внутр. справ, 2019. С. 368–370.

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

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

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

194. Романенко Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. P. 129–135. (Словацька Республіка).

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

196. Романенко 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.

197. Романенко 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 листопада 2020 р.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ: Нац. акад. внутр. справ, 2020. С. 296–298.

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

199. Романюк Б. В., Гавловський В. Д., Гуцалюк М. В., Бутузов В. М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій. Київ: Вид. Поливода А. В., 2004. 144 с.

200. Руденко І. О. Обман як спосіб вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Юридична наука: проблеми та перспективи розвитку*: матеріали Всеукр.

студентського круглого столу (Київ, 9 жовтня 2018 р.); відп. ред.: А. Ю. Олійник, О. С. Шморгун. Київ: КНУТД, 2018. С. 107–110.

201. Салтевський М. В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2006. 588 с.

202. Салтевський М. В. Криміналістика: підручник: у 2 ч. Харків: Консум, 2000. Ч. 2. 2001. 528 с.

203. Салтевський М. В., Лукашевич В. Г., Глібко В. М. Навчально-довідковий посібник з криміналістики. Київ: ВІПОЛ, 1994. 180 с.

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

205. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект: навч.-метод. посіб. Одеса, 2020. 133 с.

206. Самойленко О. А. Типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі. *Наукові праці Національного університету «Одеська юридична академія».* Т. 23. Одеса: Гельветика, 2019. С. 121–128.

207. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Донецьк, 2014. 18 с.

208. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Донецьк, 2014. 226 с.

209. Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки. *Проблеми правознавства та правоохоронної діяльності.* 2014. № 4. С. 25–31. URL: http://nbuv.gov.ua/UJRN/pppd_2014_4_6

210. Севідов О. А. Криміналістична класифікація суб'єктів кіберзлочинів та їх особливості. *Актуальні питання розслідування кіберзлочинів*: матеріали Міжнар. наук.-практ. конф. (Харків, 10 груд. 2013 р.) / МВС України, Харк. нац. ун-т внутр. справ. Харків: ХНУВС, 2013. С. 164–169.

211. Селиванов Н. А. Криминалистические характеристики преступлений и следственные ситуации в методике расследования пре ступлений. *Социалистическая законность*. 1977. № 2. С. 56–59.

212. Семеногов В. В. Проблеми висунення слідчих версій при розслідуванні вбивств прихованих інсценуванням. *Теорія і практика судової експертизи і криміналістики.* 2013. Вип. 9. С. 77–84.

213. Синчук О. В. Типові версії в структурі криміналістичної методики: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Харків, 2010. 209 с.

214. Скільки українців стали жертвами інтернет-шахрайства? *Кіберполіція.* URL: https://dyvys.info/2020/11/11/skilky-ukrayintsiv-staly-zhertvamy-internet-shahrajstva-kiberpolitsiya/

215. Скригонюк М. І. Криміналістика: навч. посіб. Київ: Київ. ун-т, 2004. 518 с.

216. Словник української мови: в 11 т. 1974. Т. 5. URL: http://sum.in.ua/s/ obstanovka

217. Сокиран Ф. М. Сучасні концепції психологічного впливу на досудовому слідстві: монографія / за заг. ред. В. Г. Гончаренка. Київ: НАВСУ, Правник, 2002. 172 с.

218. Сорокевич А. Б. Тактические приемы применения звукозаписи в допросе подозреваемых и обвиняемых. *Криминалистика и судебная экспертиза*. Киев, 1972. Выпуск 9. С. 61–67.

219. Софілкан О. В. Актуальні проблеми судово-економічної експертизи у кримінальних провадженнях про економічні злочин. *Вісник Академії адвокатури України.* 2013. Вип. 1. С. 169–174.

220. Стахівський С. М. Слідчі дії як основні засоби збирання доказів : наук.–практ. посіб. Київ : Атіка, 2009. 64 с.

221. Стахівський С. М. Кримінально-процесуальні засоби доказування : дис. ... докт. юрид. наук : 12.00.09 «Кримінальний процес та криміналістика; судова експертиза». Київ, 2005. 367 с.

222. Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека.* 2013. № 3 (50). С. 110–115.

223. Стрільців О. М., Вакуленко О. В., Тарасенко О. С. та ін. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рек. Київ: Нац. акад. внутр. справ, 2016. 56 с.

224. Стрільців О. М., Крижна В. В., Максименко О. В. та ін. Особливості розслідування кримінальних правопорушень, пов’язаних із розповсюдженням у мережі Інтернет забороненого контенту: метод. рек. / за заг. ред. Ю. Ю. Орлова. Київ: Нац. акад. внутр. справ, 2014. 80 с.

225. Стрільців О. М., Кузьмічова-Кисленко І. В., Лащук О. В. та ін. Розслідування незаконного збуту наркотичних засобів та психотропних речовин: посібник. Київ: Нац. акад. внутр. справ, 2019. 135 с.

226. Стрільців О. М., Тарасенко О. С., Курилін І. Р. та ін. Розслідування злочинів, пов’язаних з незаконним розповсюдженням у мережі Інтернет медійного контенту провайдерами програмних послуг та Інтернет-провайдерами: метод. рек. Київ: Нац. акад. внутр. справ, 2017. 44 с.

227. Схеми «Out-of-OLX» шахрайства + інфографіка. URL: https://www.ema.com.ua/citizens/cyber-safety-school/shemi-out-of-olx-shahrajstva-infografika/

228. Тарарака В. Д. Архітектура комп’ютерних систем: навч. посіб. Житомир: ЖДТУ, 2018. 383 с.

229. Тарасенко О. С., Гуцалюк М. В., Гавловський В. Д. та ін. Розслідування кримінальних правопорушень, вчинених у сфері захисту інтелектуальної власності з використанням мережі Інтернет: метод. рек. 2-ге вид., доповн. Київ: Міжвід. наук.-дослід. центр з проблем б-би з орг. злоч. при РНБО України; Нац. акад. внутр. справ, 2021. 74 с.

230. Тарасенко О. С., Федоренко О. А., Стрільців О. М. та ін. Пошук кримінально значимої інформації в мережі Інтернет: метод. рек. / за ред. Ю. Ю. Орлова. К.: Нац. акад. внутр. справ, 2020. 100 с.

231. Тарасова О. В. Об’єкт шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Право і суспільство.* 2013. № 1. С. 106–111.

232. Таций В. Я. Об'єкт і предмет злочину в кримінальному праві України: монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків: Право, 2016. 256 с.

233. Тертышник В. М., Слинько С. В. Теория доказательств: учеб. пособ. Харьков: Арсіс, 1998. 256 с.

234. Тищенко Є. Ф. Розслідування комп’ютерних злочинів: наук.-метод. посіб. Київ: Вид-во НА СБУ, 2010. 124 с.

235. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів: монографія. Одеса, Фенікс, 2007. 260 с.

236. Ткач О. В. Слідова картина як джерело доказової інформації при розслідуванні порушення недоторканності приватного життя. *Вісник кримінального судочинства.* 2015. № 4. С. 192–197.

237. Топ-5 новин в сфері шахрайства з платіжними інструментами. URL : https://pingvin.pro/gadgets/article-gadget/top-5-novyn-v-sferi-shahrajstva-z-platizhnymy-instrumentamy-13.html

238. Уголовный кодекс Украины : науч.-практ. коммент. / отв. ред. Е. Л. Стрельцов. 6-е изд., перераб. и доп. Харьков : Одиссей, 2009. 888 с.

239. Удалова Л. Д., Письменний Д. П., Азаров Ю. І. та ін. Теорія судових доказів у питаннях і відповідях: навч. посіб. Київ: Центр учбової літератури, 2015. 104 с.

240. Удовенко Ж. В. Криміналістика: конспект лекцій / ред. В. І. Галаган. Київ: Центр учб. літ., 2016. 320 с.

241. Фріс П. Л. Кримінальне право України. Загальна частина: підруч. для студ. вищих навч. закл. 2-ге вид., доповн. і перероб. Київ: Атіка, 2009. 512 с.

242. Фулей Т. І. Застосування практики Європейського суду з прав людини при здійсненні правосуддя: наук.-метод. посіб. для суддів. 2 вид. випр., допов. Київ, 2015. 208 с.

243. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України. Київ: Істина, 2004. 504 с.

244. Хижняк Є. С. Типові слідчі ситуації при розслідуванні статевих злочинів. *Південноукраїнський правничий часопис.* 2012. № 4. С. 197–199.

245. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. URL: https://zakon. rada. gov. ua/cgi-bin/laws/main. cgi? nreg=435-15.

246. Цільмак О. М. Основи побудови криміналістичних версій *Порівняльно-аналітичне право.* 2014. № 2. С. 334–338.

247. Цуцкірідзе М. С., Мельничук В. М., Стрільців О. М., Стародуб С. П. Виявлення та досудове розслідування кримінальних правопорушень, пов’язаних із фальсифікацією лікарських засобів або обігом фальсифікованих лікарських засобів: метод. рек. Київ: ГСУ МВС України, Нац. акад. внутр. справ, 2013. 92 с.

248. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства: автореф. дис. ... докт. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2010. 34 с.

249. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства: дис. ... докт. юрид. наук: 12.00.09.

«Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2010. 610 с.

250. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ. нац. ун-т внутр. справ. Київ: Хай-Тек Прес, 2010. 623 с.

251. Чорноус Ю. М. Актуальні питання створення і діяльності міжнародних спільних слідчих груп. *Криминалист первопечатный.* Харків, 2017. № 14. С. 36–47.

252. Чорноус Ю. М. Міжнародна злочинність: актуальні завдання для криміналістичної методики. *Наукові праці Національного університету «Одеська юридична академія».* 2017. Т. XIX. С. 421–429.

253. Чучко С. В. Віртуальні (комп'ютерні) сліди шахрайства, пов'язаного із торгівлею товарами через мережу Інтернет. *Сучасні інформаційні технології в діяльності Національної поліції України:* матеріали Всеукр. наук.-практ. семінару (Дніпро, 26 листоп. 2020 р.). Дніпро: ДДУВС, 2020. С. 25–28.

254. Шавиркін Б. В. Деякі особливості розслідування кіберзлочинів. *Боротьба з інтернет-злочинністю* : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). Донецьк: Донец. юрид. ін-т, 2013. С. 124–128.

255. Шамара О. В., Бантишев О. Ф., Чорний Р. Л. Протидія терористичній діяльності (кримінально-правові аспекти): монографія. Київ: НА СБ України, 2011. 160 с.

256. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 1. С. 145–149.

257. Шевчук В. М. Слідчі ситуації та їх вплив на розробку тактичних операцій. *Науковий вісник Міжнародного гуманітарного університету*. 2013. № 6–3. Т. 2. С. 125–129.

258. Шепітько В. Ю. Допит: наук.-практ. посіб. Харків: КримАрт, 1998. 33 с.

259. Шепітько В. Ю. Криміналістика. Енциклопедичний словник (український–російський і російський–український) / за ред. В. Л. Тація. Харків: Право, 2001. 560 с.

260. Шепітько М. В. Спосіб вчинення злочину *як* ознака складу злочинів проти правосуддя. *Форум права.* 2015. № 4. С. 330–335.

261. Щербаковский М. Г., Кравченко А. А. Применение специальных знаний при раскрытии и расследовании преступлений: учеб. пособ. Харьков: ХНУВС, 1997. 76 с.

262. Эйсман А. А. Заключение эксперта. Структура и научное обоснование. Москва: Юрид. лит., 1967. 152 с.

263. Энциклопедия судебной экспертизы / под ред. Т. В. Аверьяновой, Е. Р. Росинской. Москва: Юрист, 1999. 552 с.

264. Юсупов В. В. Криміналістика в Україні у XX–XXI століттях: монографія. Київ: ФОП Маслаков, 2018. 556 с.

265. Якупов А.Ш. Уголовное право УССР: учебник. Киев: Вища шк., 1984. 384 с.

266. Янковий М. О. Генезис поняття та сутність допиту. *Науковий вісник Київського національного університету внутрішніх справ.* 2007. Вип. 5. С. 185–191.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

праці, в яких опубліковано основні наукові результати дисертації:

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

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

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

4. Романенко (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.

5. Романенко (Коршикова) Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. P. 129–135. (Словацька Республіка).

праці, які засвідчують апробацію матеріалів дисертації:

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

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

7. Романенко (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.

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

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

які додатково відображають наукові результати дисертації

10. Тарасенко О. С., Федоренко О. А., Стрільців О. М. та ін. Пошук кримінально значимої інформації в мережі Інтернет: метод. рек. / за ред. Ю. Ю. Орлова. К.: Нац. акад. внутр. справ, 2020. 100 с.

Додаток Б

Результати
зведених даних анкетування 300 слідчих підрозділів досудового розслідування Національної поліції України у зв'язку з дослідженням проблем розслідування шахрайства, учиненого з використанням електронно-обчислювальної техніки

В анкетуванні взяли участь 50 слідчих Головного управління Національної поліції у м. Києві, а також 250 слідчих з усіх регіонів України, які проходили підвищення кваліфікації у Національній академії внутрішніх справ у період 2019–2020 років. Предметом анкетування було дослідженням проблем розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки.

Запитання	Результат	
	300 осіб	%
1. Ваша посада:		
а) начальник слідчого підрозділу	25	8,3
б) заступник начальника слідчого підрозділу	21	7,0
в) старший слідчий в ОВС	60	20,0
г) старший слідчий	104	34,6
д) слідчий	90	30,0

2. Стаж роботи у слідчих підрозділах:		
а) до 2 року	55	18,3
б) до 5 років	202	67,3
в) до 10 років	29	9,7
г) понад 10 років	14	4,7

3. Який територіальний орган Національної поліції представляєте:		
а) міський	10	3,3
б) районний у місті	84	28,0
в) районний	206	68,7

4. Чи розслідували Ви особисто кримінальні провадження щодо шахрайства, учиненого з використанням електронно-обчислювальної техніки?		
а) так	174	58,0
б) ні	126	42,0

5. На Вашу думку, первинна інформація про шахрайства,		

учинені з використанням електронно-обчислювальної техніки, є результатом:		
а) оперативно-розшукової діяльності оперативних підрозділів	12	4,0
б) слідчої діяльності в рамках кримінального провадження	9	3,0
в) заяви та повідомлення громадян	251	83,7
г) не можу зазначити	28	93,3

6. На Вашу думку, що може бути предметом шахрайств, учинених з використанням електронно-обчислювальної техніки (можлива будь-яка кількість відповідей)?		
А) майно (рухоме та не рухоме)	114	38,0
Б) право на майно	21	7,0
В) кошти	234	78,0
Г) інформація	7	2,3
д) невідомо	16	5,3

7. На Вашу думку, які способи використовуються для заволодінням майном під час шахрайств, учинених з використанням електронно-обчислювальної техніки (можлива будь-яка кількість відповідей)?		
а) отримання у власників платіжних карток реквізитів та іншої конфіденційної інформації про картки (фішинг)	214	71,3
б) створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих товарів	9	3,0
в) отримання даних про банківську картку з використанням ЕОТ	72	24,0
г) створення або використання сайтів благодійних організацій	17	5,7
д) заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину (для прикладу, OLX)	163	54,3
е) створення та діяльність фіктивних фінансових бірж	3	1,0
є) інші способи	1	0,3
ж) невідомо	39	13,0

8. Які види слідів найчастіше можуть залишатися в результаті розслідування шахрайства, учиненого з використанням електронно-обчислювальної техніки (можлива будь-яка кількість відповідей)?		
а) інформаційні сліди, що утворюються на ЕОТ, якою користувався злочинець під час створення повідомлень, адміністрування сайтів та електронної переписки	215	71,7
б) інформаційні сліди, що утворюються на сайтах та у	256	85,3

соціальних мережах		
в) інформаційні сліди, що утворюються під час електронної переписки злочинця	251	83,7
г) інформаційні сліди, що утворюються у засобах зв'язку під час спілкування злочинця	198	66,0
д) інформаційні сліди, що утворюються на інших засобах телекомунікації, які використовував злочинець під час створення повідомлень, адміністрування сайтів та електронної переписки	211	70,3
е) телефонний трафік між злочинцем і потерпілим	202	67,3
є) сліди пальців рук на ЕОТ та інших пристроях, якими користувався злочинець	154	51,3
ж) сліди пальців рук на засобах зв'язку злочинця	127	42,3
з) сліди пальців рук на предметах, отриманих в результаті шахрайства	200	66,7
і) мікрочастини на ЕОТ та інших пристроях, якими користувався злочинець	178	59,3
и) мікрочастини на засобах зв'язку, якими користувався злочинець	189	63,0
к) мікрочастини на предметах, отриманих в результаті шахрайства	76	25,3
л) відеоматеріали, що засвідчують перебування злочинця в громадських місцях під час створення повідомлень, адміністрування сайтів та електронної переписки на інших засобах телекомунікації, які використовував для цього злочинець	44	14,7
м) сліди, що утворюються під час переказу коштів потерпілим злочинцю	131	43,7
н) сліди, що утворюються під час отримання у банківських установах готівки злочинцем	154	51,3
о) інші види слідів	3	1,0

9. Де можуть бути виявлені сліди шахрайства, учиненого з використанням електронно-обчислювальної техніки (можлива будь-яка кількість відповідей)?		
а) електронна поштова скринька (віртуальні сліди у вигляді переписки з питань створення та поширення інформації)	215	71,7
б) інтернет-сайт (сліди створення та адміністрування певного сайту)	255	85,0
в) профіль у соціальних мережах (під яким був зареєстрований злочинець)	149	49,7
г) рахунок в електронних платіжних системах (на який переказувались кошти потерпілого)	102	34,0

д) база даних телефонного трафіку (абонентів операторів зв'язку та ін.)	154	51,3
е) локальна мережа Інтернет (в яку виходив злочинець)	289	96,3
є) електронно-обчислювальна техніка (віртуальні сліди, сліди пальців рук і мікрочастин)	278	92,6
ж) засоби телекомунікації, що належать злочинцю (сліди пальців, мікрочастини та віртуальні сліди)	251	83,7
з) засоби телекомунікації, що належать іншим фізичним та юридичним особам (віртуальні сліди)	121	40,3
і) відеозаписи, що належать іншим фізичним та юридичним особам (під час перебування злочинця у таких приміщеннях під час входження у мережу Інтернет)	119	39,7
ї) інші види слідів	2	0,7

10. Які версії можуть висуватися щодо особи при виявленні факту шахрайства, учиненого з використанням електронно-обчислювальної техніки?		
а) шахрайство з використанням ЕОТ вчинене особою (групою осіб), щодо якої є первинна інформація або особу злочинця, визначено чи є достатньо даних для її встановлення	113	37,7
б) шахрайство з використанням ЕОТ вчинене невідомою особою (групою осіб)	292	97,3
в) інші _____	1	0,3

11. Які версії, на Вашу думку, можуть висуватися щодо місця розташування ЕОТ, з якого злочинці вчиняли шахрайство (можлива будь-яка кількість відповідей?		
а) ЕОТ розташована на території України	201	67,0
б) ЕОТ розташована за межами території України	183	61,0
в) ЕОТ розташована на тимчасово окупованій території у Донецькій та Луганській областях або анексованій Автономній Республіки Крим	239	79,7
г) інші_____	5	1,7

12. Які процесуальні дії, на Вашу думку, найчастіше проводяться під час досудового розслідування шахрайства, учиненого з використанням електронно-обчислювальної техніки (не більше п'яти відповідей)		
а) огляд місця події – робоче місце потерпілого	106	35,3
б) обшук місця знаходження ЕОТ, з використанням якої здійснювалось шахрайство	298	99,3
в) особистий обшук затриманої особи	121	40,3
г) обшук житла чи іншого володіння підозрюваного	189	63,0

д) затримання підозрюваного	300	100,0
е) допит підозрюваного	300	100,0
є) одночасний допит двох і більше вже допитаних осіб	37	12,3
ж) допит свідків	56	18,6
з) отримання зразків для експертизи	2	0,6
і) призначення експертиз	278	92,7
ї) тимчасовий доступ до речей і документів	151	50,3
и) пред'явлення особи для впізнання	33	11,0
к) пред'явлення речей для впізнання	153	51,0
л) слідчий експеримент	4	1,3
м) освідування особи	7	2,3
н) негласні слідчі (розшукові) дії	148	49,3
о) наведення довідок	111	37,0

13 Які тактичні прийоми Ви пропонуєте використовувати під час допиту підозрюваного у вчинені шахрайства з використанням ЕОТ (може бути декілька відповідей)?		
а) пред'явлення особі, яку допитують, речових доказів та інших матеріалів провадження, що свідчать про користування нею певною ЕОТ, створення та подальше адміністрування вебпорталом (сайтом), здійснення електронної переписки з потерпілим (або здійснення телефонних переговорів), або спростовують її алібі	287	95,7
б) оголошення показань інших підозрюваних, потерпілих, свідків	181	60,1
в) використання суперечностей у самих показаннях допитуваного або з іншими доказами	75	25,0
г) максимальна деталізація показань з метою виявлення суперечностей	49	16,3
д) пропозиція повторного викладення показань про подію загалом або окремі її обставини	41	13,7
е) вияв розуміння становища, в якому опинилася особа, яку допитують	36	12,0
є) переконання в необхідності повідомлення правдивих відомостей	14	4,7
ж) спонукання до каяття шляхом формування внутрішнього протесту проти вчинених дій	7	2,3
з) інше	2	0,3

14 Чи необхідна, на Вашу думку, обов'язкова присутність спеціаліста під час проведення обшуку у підозрюваного при розслідуванні шахрайств, учинених з використанням електронно-обчислювальної техніки?		
а) так	198	66,0

б) ні	99	33,0
в) важко відповісти	3	1,0

15 Які експертизи доцільно назначати при розслідуванні шахрайств, учинених з використанням електронно-обчислювальної техніки (можлива будь-яка кількість відповідей)?		
а) експертиза комп'ютерної техніки і програмних продуктів (комп’ютерно-технічна експертиза) щодо ЕОТ, програмних продуктів	300	100,0
б) експертиза телекомунікаційних систем і засобів	275	91,7
в) дактилоскопічна експертиза щодо вилучених слідів рук з різних предметів (ЕОТ, телекомунікаційних систем і засобів, грошей, майна, документів тощо)	258	86,0
г) експертиза матеріалів і засобів звукозапису щодо записів дій та переговорів злочинця, а також щодо технічних засобів знімання та фіксації такої інформації	141	47,0
д) експертиза документів бухгалтерського, податкового обліку і звітності	22	7,3
е) судово-психіатрична експертиза підозрюваного	299	99,7
є) судово-наркологічна експертиза підозрюваного	202	67,3
ж) інші _____	2	0,7

16 На Вашу думку, чи є специфіка в розслідуванні шахрайств, учинених з використанням електронно-обчислювальної техніки, що дозволяє виділити їх в окрему методику розслідування?		
а) так	261	87,0
б) ні	15	5,0
в) важко відповісти	24	8,0

Додаток В

Результати
зведених даних вивчення 40 кримінальних проваджень у зв'язку з дослідженням проблем розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки
(ч. 3 ст. 190 КК України)

1. Місцезнаходження ЕОТ, яка використовувалася для вчинення шахрайства:		
Всього:	**40**	**100%**
а) територія України	40	100,0
б) територія інших держав	0	0
в) тимчасово окуповані території Донецької та Луганської областей або анексованої Автономної Республіки Крим	0	0
г) не встановлено	0	0

2. Спосіб вчинення шахрайства з використанням ЕОТ:		
Всього фактів	**100**	**%**
а) отримання у власників платіжних карток реквізитів та іншої конфіденційної інформації про картки (фішинг)	1	2,5
б) створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих товарів	0	0
в) отримання даних про банківську картку з використанням ЕОТ	0	0
г) створення або використання сайтів благодійних організацій	0	0
д) заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину (для прикладу, OLX.ua)	39	97,5
е) створення та діяльність фіктивних фінансових бірж	0	0
є) інші способи		

3. Предмет шахрайства, яке вчинялось з використанням ЕОТ		
а) майно (рухоме та нерухоме)	9	22,5
б) право на майно	0	0
в) кошти	31	77,5
г) інформація	0	0

4. Предмети та сліди, які були виявлені під час розслідування шахрайства, учиненого з використанням ЕОТ:			
а) Електронно-обчислювальна техніка	Комп’ютер	40	100
	Ноутбук	5	12,5
	Планшет	3	7,5
	Інше	1	2,5
б) безперебійник		33	82,5
в) принтер		21	52,5
г) МФУ		2	5,0
д) сканери		5	12,5
е) навушники		7	17,5
є) адаптер (передавач) WI-FI		40	100,0
ж) флеш-пам'ять		40	100,0
з) оптичні диски (CD, DVD)		4	10,0
і) зовнішні HDD		3	7,5
ї) телефон		40	100,0
и) кошти		40	100,0
к) майно (речі), яке отримано злочинним шляхом		2	5,0
л) банківські картки		37	92,5
м) інше		2	5,0

5. Характеристика особи злочинця (всього 40 осіб):		
5.1. Стать:		
а) чоловіки – всього:	40	
б) жінки – всього:	0	
5.2. Громадянство:		
а) України:	100	
б) інших країн:	0	
5.3. Вік:		
а) до 18 років:	0	0
б) від 18 до 25 років	13	32,5
в) від 25 до 35 років:	24	60,0
г) від 35 до 45 років	3	7,5
д) понад 45 років	0	0

5.4. Освіта:		
а) неповна середня	0	
б) середня	7	17,5
в) середня спеціальна	5	12,5
г) незакінчена вища	18	45,0
д) вища	10	25,0

5.5. Сімейний стан:

а) одружений (-а)	14	35,0
б) не одружений (-а)	26	65,0
в) вдовець (-ва)	0	0
г) цивільний шлюб	0	0
д) розлучений (-а)	0	0

5.6. Рід занять:		
а) не працює і не навчається:	33	82,5
б) навчається	5	12,5
в) офіційно працевлаштовані	2	5,0

5.7. Досвід злочинної діяльності:		
а) несудимий	38	95,0
б) один раз судимий	2	5,0
в) два і більше рази судимий	0	

6. Джерела інформації, що слугували підставою для відкриття кримінального провадження про вчинення шахрайства, з використанням ЕОТ:		
а) повідомлення фізичних або юридичних осіб	40	100
б) самостійно виявлені слідчим за результатами кримінального провадження	0	0
в) результати оперативно-розшукової діяльності	0	0
г) інші джерела повідомлень	0	0

7. Види експертиз, які призначалися при розслідуванні шахрайств, учинених з використанням електронно-обчислювальної техніки:		
а) експертиза комп'ютерної техніки і програмних продуктів (комп’ютерно-технічна експертиза) щодо ЕОТ, програмних продуктів	40	100,0
б) експертиза телекомунікаційних систем і засобів	40	100,0
в) дактилоскопічна експертиза щодо вилучених слідів рук з різних предметів (ЕОТ, телекомунікаційних систем і засобів, грошей, майна, документів тощо)	5	12,5
г) експертиза матеріалів і засобів звукозапису щодо записів дій та переговорів злочинця, а також щодо технічних засобів знімання й фіксації такої інформації	0	0
д) експертиза документів бухгалтерського, податкового обліку і звітності	0	0
е) судово-психіатрична експертиза підозрюваного	40	100,0
є) судово-наркологічна експертиза підозрюваного	1	2,5
і) інші _____		

Додаток Г

Акти впровадження

ЗАТВЕРДЖУЮ
Перший проректор
Національної академії
внутрішніх справ,
доктор юридичних наук, професор
заслужений юрист України

Станіслав ГУСАРЄВ
21 04 2021 р.

АКТ
про впровадження у освітній процес Національної академії внутрішніх справ результатів дисертації ад'юнкта кафедри криміналістики та судової медицини НАВС Романенко Тетяни Василівни на тему «Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки» подану на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі: начальника навчально-методичного відділу Колодейчак С.І. (голова комісії), завідувача наукової лабораторії з проблем протидії злочинності навчально-наукового інституту № 1, доктора юридичних наук, професора Вознюка А.А., завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента Самодіна А.В., склала цей акт про те, що результати дисертації Романенко Тетяни Василівни на тему «Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки» впроваджені у освітній процес академії.

На основі проведеного аналізу комісія дійшла висновку, що подані наукові праці Романенко Т.В. містять науково обґрунтовані теоретичні положення і практичні рекомендації, запроваджені для використання в освітньому процесі Національної академії внутрішніх справ, зокрема у системі професійної освіти слідчих, підвищення кваліфікації поліцейських, при викладанні відповідних навчальних дисциплін та під час підготовки навчальних і методичних посібників, підручників, курсів лекцій.

Голова комісії: **Станіслава КОЛОДЕЙЧАК**

Члени комісії:
доктор юридичних наук, професор **Андрій ВОЗНЮК**

кандидат юридичних наук,
доцент **Артем САМОДІН**

«ЗАТВЕРДЖУЮ»
Заступник начальника
Головного слідчого управління
Національної поліції України,
кандидат юридичних наук
полковник поліції

Руслан ДУДАРЕЦЬ

28 січня 2021 року

А К Т
впровадження у практичні діяльність органів досудового розслідування матеріалів дисертаційного дослідження здобувача Національної академії внутрішніх справ Тетяни Романенко «Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки»

Комісія у складі: начальника відділу ГСУ НП України Бурлака В.В., старшого слідчого в особливо важливих справах ГСУ НП України, кандидата юридичних наук Карпенко Н.В., старшого слідчого в особливо важливих справах ГСУ НП України, кандидата юридичних наук Дубівки І.В., склала цей акт про те, що матеріали дисертаційного дослідження здобувача Національної академії внутрішніх справ Тетяни Романенко «Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки» можуть застосовуватись у практичній діяльності слідчих підрозділів, а також під час проведення занять в системі службової підготовки.

Начальник відділу
Головного слідчого управління
Національної поліції України **Владислав БУРЛАКА**

Старший слідчий в ОВС ГСУ
Національної поліції України
кандидат юридичних наук **Наталія КАРПЕНКО**

Старший слідчий в ОВС ГСУ
Національної поліції України
кандидат юридичних наук **Ірина ДУБІВКА**