УДК 343.98
DOI https://doi.org/10.32849/2663-5313/2020.12.45

Ілля Коваленко,
адвокат,
аспірант кафедри криміналістики та домедичної підготовки
Дніпропетровського державного університету внутрішніх справ

ОКРЕМІ ВИДИ ЕКСПЕРТИЗ ЯК ОБОВ'ЯЗКОВІ СЛІДЧІ (РОЗШУКОВІ) ДІЇ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Стаття висвітлює проблематику дослідження видів комп'ютерно-технічних експертиз, що являються обов'язковими слідчими (розшуковими) діями у розслідуванні злочинів із залученням новітніх технологій та комп'ютерних систем, таких як шахрайство у сфері банківських електронних платежів. У ній наголошено та тому, що для більш якісного розкриття таких складних кримінальних правопорушень база знань експертів та їх методичне забезпечення весь час повинні поновлюватись та йти на випередження, адже щосекунди у світі з'являються нові технології та викрадаються сотні тисяч доларів США щодня. Розглянуто найбільш поширені технічні засоби, девайси та програмне забезпечення, які необхідно дослідити експерту у рамках судової комп'ютерно-технічної експертизи. Запропонована послідовність дій експерта під час дослідження обчислювальної техніки для виявлення слідів кримінальних правопорушень, а також проаналізовано думки сучасних науковців, що вивчали дане питання. Пропонується розділити експертизу техніки, що використовувалась для вчинення шахрайства, на чотири етапи згідно з видами судової комп'ютерно-технічної експертизи, а саме почати дослідження з визначення апаратних засобів, потім встановлення програмного забезпечення, виявлення інформації і, наостанок, визначення мережевих слідів зловмисників. Велику увагу було приділено визначенню основних апаратних засобів, що повинні бути дослідженими експертами. Визначено предмет, завдання, а також актуальні питання щодо кожного з видів судової комп'ютерно-технічної експертизи. Також було наголошено на важливості співпраці державних правоохоронних органів України з міжнародними партнерами та експертами задля досягнення спільної мети розкриття шахрайства у сфері банківських електронних платежів, а також на необхідності швидкої комунікації між відомствами різних країн. Наголошено на проблемі компетентності експертів у сфері інформаційних технологій та комп'ютерних систем, матеріально-технічного забезпечення, а також застарілого програмного забезпечення для проведення судової комп'ютерно-технічної експертизи.

Ключові слова: судова комп'ютерно-технічна експертиза, інтернет-банкінг, інформаційні технології, сліди злочину, кіберзлочин.

Постановка проблеми. 21-е століття можна впевнено назвати «комп'ютерним століттям». Стрімкий розвиток інформаційних технологій полегшив життя людства та, у свою чергу, породив нові кримінальні правопорушення у сфері інформаційних технологій. Всесвітня мережа Інтернет стала для всього людства невід'ємною частиною життя. За допомогою Інтернету люди спілкуються у всьому світі за допомогою соціальних мереж, месенджерів. Ще 20 років тому це було практично нереально, сьогодні – це звичайні речі. Ці зміни також стосуються і банківського сектору. Зокрема, для того, щоб провести платіж, здебільшого використовується Internet banking. Тобто для того, щоб оплатити будь-які послуги, не потрібно йти у відділення банку – це все можна зробити за декілька секунд, маючи доступ до Інтернету. Незважаючи на масу переваг, ця ситуація активізувала спалах вчинення кримінальних правопорушень, кількість яких збільшуються щорічно, зокрема шахрайство у сфері банківських електронних платежів. Такі кримінальні правопорушення, як правило, кваліфікуються за ч. 3 ст. 190 КК України [1], а під час їх розслідування призначається комп'ютерно-технічна експертиза.

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

думок вчених, які досліджували проблематику даного питання.

Аналіз останніх досліджень і публікацій. У криміналістичній літературі загальним питанням проведення судових експертиз приділялася увага в роботах Н.Т. Малаховської, А.І. Вінберга, О.Р. Шляхова, М.В. Салтевського, М.О. Селіванова, Г.Л. Грановського. Теоретичними засадами призначення та проведення комп'ютерно-технічних експертиз у провадженнях про економічні та фінансові кримінальні правопорушення, до яких належить шахрайство у сфері використання банківських електронних платежів, займалися А.І. Усов, Б.К. Давлєтов, О.Р. Росинська, Д.В. Пашнєв, В.Б. Вєхов та ін.

Але комплексного аналізу щодо видів комп'ютерно-технічної експертизи під час розслідування шахрайства у сфері використання банківських електронних платежів вченими не проводилося. Водночас на практиці виникає потреба в науково-обґрунтованих криміналістичних рекомендаціях щодо проведення комп'ютерно-технічних експертиз у розрізі розслідування досліджуваної категорії кримінальних правопорушень.

Мета дослідження. Метою статті є дослідження видів комп'ютерно-технічних експертиз як обов'язкових слідчих (розшукових) дій під час розслідування шахрайства у сфері банківських електронних платежів, особливостей призначення й проведення у кримінальному судочинстві, а також виокремлення їх проблемних аспектів.

Виклад основного матеріалу. Одною з основних процесуальних дій у розслідуванні шахрайства у сфері банківських електронних платежів є призначення судової експертизи, а саме судової комп'ютерно-технічної експертизи, яка проводиться відповідно до ст. 242 КПК України [2].

Судова комп'ютерно-технічна експертиза (далі по тексту – СКТЕ) призначається у разі, коли необхідно отримати фактичні дані для розслідування кіберзлочинів з використанням електронно-обчислюваної техніки, якими є факти вчинення шахрайства у сфері банківських електронних платежів, для створення доказової бази в кримінальних провадженнях.

Ефективність розслідування кримінальних правопорушень, таких як шахрайство у сфері банківських електронних платежів, залежить від своєчасного виявлення слідів кримінального правопорушення, адже у разі, якщо слідчі (розшукові) дії будуть проведені невчасно та із запізненням, зловмисники можуть знищити всю доказову базу, а саме виконати форматування жорсткого диску, фізичне знищення жорсткого диску за допомогою мікрохвильової печі, USB-накопичувачів, зовнішніх накопичувачів, CD-, DVD-дисків тощо. Для того щоб сліди, які знаходяться на електронних носіях, стали доказами, їх необхідно знайти, виявити та зафіксувати процесуальним шляхом, що регулюється ЗУ «Про судову експертизу» [3].

Комп'ютерно-технічна експертиза – це підвид інженерно-технічної експертизи [4], за якої досліджуються певні технічні характеристики обчислювальної техніки, а саме стаціонарних комп'ютерів (ПК), смартфонів, ноутбуків, планшетів, нетбуків тощо, та проводиться детальний аналіз програм, встановлених на даних технічних засобах, з метою виявлення інформації, що знаходиться в електронному вигляді на даних пристроях, для встановлення факту скоєння кримінального правопорушення. За допомогою експертизи виявляються ознаки кримінального правопорушення, що слугують створенню доказової бази шляхом аналізу виявленої інформації [5].

Факти та обставини, що виявляються в процесі аналізу апаратно-технічних засобів та програмного забезпечення, встановленого на цих засобах, які є доказами у матеріалах кримінального провадження, є предметом СКТЕ [6, с. 118-119].

Як зазначає А. І. Усов, залежно від обставин кримінального провадження можуть бути призначені такі види експертиз:

– апаратно-комп'ютерна (АКЕ);
– програмно-комп'ютерна (ПКЕ);
– комп'ютерно-мережева експертиза (КМЕ);
– інформаційно-комп'ютерна (ІКЕ) [7, с. 14].

Об'єктом дослідження апаратно-комп'ютерної експертизи (далі по тексту – АКЕ) може бути саме техніка, за допомогою якої вчинялось шахрайство у сфері банківських електронних платежів. До апаратних засобів належать: електричні, електронні та механічні схеми, блоки, прилади і пристрої, що становлять матеріальну частину комп'ютерної системи. Під час проведення даної експертизи досліджуються ноутбуки, системні блоки, в яких встановлюється вид та назва процесора (CPU), вид та назва материнської плати (motherboard), вид оперативної пам'яті (RAM), назва відеокарти (GPU), вид жорсткого накопичувача (HDD або SSD). Встановлення видів і назв технічних засобів дозволяє порівняти їх зі слідами, залишеними злочинцем на серверах банківських установ або організацій, що під-

далися шахрайським діям. Головним ідентифікаційним фактором комп'ютера, з якого проводились шахрайські дії, є так званий ідентифікаційний номер ПК (MAC-адреса). MAC-адреса (Media Access Control, адреса управління доступом до середовища) записується в заводську прошивку мережевого адаптера під час його виготовлення [8]. Він потрібен для того, щоб ідентифікувати конкретний мережевий адаптер, який знаходиться на материнській платі. Кожен пакет даних, що приймається адаптером, містить його MAC-адресу, для того щоб пристрій міг зрозуміти, що ці дані призначені саме йому. MAC-адреса ПК подібна відбиткам пальців, якщо злочинець, вчиняючи шахрайські операції у сфері банківських електронних платежів, був необережний у своїх діях та не замінив MAC-адресу за допомогою спеціальних програм, то його обчислювана техніка, за допомогою якої шахрай вчинив суспільно небезпечне діяння, буде ідентифікована.

Проводячи АКЕ, експерт повинен зупинитися на таких моментах:

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

– визначити тип, марку або модель даного пристрою;

– встановити технічні характеристики і параметри досліджуваного технічного засобу;

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

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

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

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

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

Завданням ПКЕ є встановлення наявності певних видів програм, що сприяють вчиненню шахрайських операцій у сфері банківських електронних платежів. Ними можуть бути програми, призначені для віддаленого доступу до інформації та керування комп'ютером, наприклад: AnyDesk, Supremo Remote Desktop, TeamViewer, RemotePC тощо. Важливою являється наявність програм, призначених для анонімного та зашифрованого спілкування в мережі Інтернет, таких як Jabber, Telegram, WhatsApp та ін. Як правило, зловмисники можуть використовувати графічні редактори для підробки документів, наприклад Adobe Photoshop, Corel Draw тощо, тому експерт повинен ідентифікувати їх наявність та встановити історію застосування таких додатків, відновити файли, створені за допомогою цих програм і, таким чином, виявити важливі сліди вчинення злочину, що можуть стати важливими доказами в кримінальному провадженні. Не менш вагомою знахідкою можуть бути програми для віддаленого керування банківськими рахунками – інтернет-банкінг, які зловмисники зазвичай використовують на смартфонах та планшетах. У разі виявлення вищезазначеного програмного забезпечення експерту потрібно встановити або відновити log-файли використання цих програм, що дозволить виявити ланцюг операцій та послідовність дій шахрая.

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

Під час виконання ІКЕ також необхідно з'ясувати, чи встановлено на техніці, що була представлена на СТКЕ, програмне забезпечення для шифрування та захисту інформації, що підтверджувала би чи спростовувала здійснення шахрайства у сфері банківських електронних платежів. Шифрування диска створює зашифровані розділи на жорстких дисках або створює віртуальні зашифровані диски у файлі [9, с. 6]. Після шифрування дані, що зберігаються в розділі, потребують доступу до пароля. Як правило, шахраї накладають одразу декілька різних паролів для унеможливлення доступу сторонніх осіб до інформації, яка може викрити їхні зловмисні дії. Кожен із таких паролів захищено за допомогою алгоритму шифрування AES 128- або 256-бітного ключа, який дуже важко і практично неможливо розшифрувати, зважаючи на щосекундний розвиток технологій і відсталість в обізнаності з новітніми комп'ютерними системами та їх використанням в сучасній криміналістиці. Найпоширенішими програмами шифрування даних станом на 2020 рік є: Folder Lock, AxCrypt, CryptoExpert, CertainSafe, VeraCrypt, TrueCrypt, Bitlocker, Ciphershed.

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

IP-адреса – це числова послідовність, яка слугує ідентифікатором девайсу для Інтернет-сервера [10, с. 5]. IP-адреса відображається у вигляді серії з чотирьох груп чисел, розділених крапками. Перша група – це число від 1 до 255, а інші групи – число від 0 до 255, наприклад 192.135.174.1. Кожен сервер має свою унікальну адресу, за допомогою якої експерти можуть визначити фізичну адресу місця, де було скоєне кримінальне правопорушення. Саме з цієї причини шахраї намагаються замаскувати такі сліди, використовуючи ряд мережевого програмного забезпечення.

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

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

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

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

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

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

Важливою проблемою в аспекті проведення СКТЕ є її науково-методичне забезпечення. Відповідно до ст. 85 Конституції України [11], Верховна Рада України вибрала стратегічний курс держави на набуття повноправного членства України в Європейському Союзі, тим самим піднявши високу планку щодо прав та свобод людини і, як наслідок, збільшивши державну відповідальність перед міжнародними партнерами. Кожній людині гарантовано дотримання правових принципів при здійсненні правосуддя та проведення експертизи, тобто будуть застосовані одні і ті ж самі методики досліджень незалежно від того, якої форми власності установа, яка проводить експертизу, або який експерт буде її проводити.

Як влучно зазначила І. В. Гора, експертна практика судово-експертних установ повинна бути єдиною як у підходах, так і в роз'ясненнях експертів. Науково-апробовані методики та наукові критерії повинні застосовуватись за єдиними стандартами [12, с. 273].

Застосування судовими експертами наукової або спеціалізованої мови з посиланням на авторські методики, наукові підходи, у зв'язку з відсутністю у суддів спеціальних знать, сприяє психологічному тиску на нього. Дана ситуація має використовуватися з метою маніпулювання судовою думкою, сфальсифікованими доказовими базами по кримінальним провадженням сторонами як обвинувачення, так і захисту [13].

Однією з головних проблем сьогодення у проведенні СКТЕ є питання підтвердження компетентності осіб, які проводять даний вид експертиз, які володіють спеціальними знаннями в галузі інформації та які не є співробітниками державних судово-експертних установ [14, с. 144].

Висновки

Для успішної боротьби з шахрайством у сфері банківських електронних платежів, поряд із розробкою методичного забезпечення для виконання експертних досліджень, необхідне проведення регулярних міжнародних зустрічей представників правоохоронних органів. Метою цих зустрічей повинна бути конкретизація основних напрямів даного виду діяльності й обмін досвідом, а також взаємодія у боротьбі як з внутрішньодержавними, так і з міжнародними злочинними групами, що спеціалізуються на злочинах у сфері інформаційних технологій.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III.URL: https://zakon.rada.gov.ua/laws/show/2341-14/page#Text (дата звернення: 07.00.2020).

2. Кримінально процесуальний кодекс України від 18.10.2019 р. № 4651-VI URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 07.00.2020).

3. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII. *Відомості Верховної Ради України*. 1994. № 28. Ст. 232.

4. Інструкція про призначення та проведення судових експертиз та експертних досліджень : затв. наказом Міністерства юстиції України від 08.10.1998 р. № 53/5 (у ред. наказу від

26.12.2012 р. № 1950/5). *Офіційний вісник України*. 2013. № 3. Ст. 91.

5. Експертна служба МВС України. URL: https://dndekc.mvs.gov.ua/ експертна-спеціальність-10-9-досліджен/ (дата звернення: 07.00.2020).

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

7. Усов А.И. Методы и средства решения задач компьютерно-технической экспертизы : учебное пособие. Москва : ГУ ЭКЦ МВД России, 2002. 200 с.

8. IEEE Standards Association (IEEE SA). URL: https://standards.ieee.org/products-services/regauth/oui36/index.html (дата звернення: 07.00.2020).

9. Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000. 274 p.

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

11. Конституція України. *Відомості Верховної Ради України (ВВР)*. 1996. № 30. С. 141.

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

13. Проблемы проведения и научного обеспечения судебных экспертиз. URL: https://ceur.ru/library/articles/ pravo/item127028 (дата звернення: 07.00.2020).

14. Карпінська Н., Крикунов О. Історико-правовий часопис. 2017. № 1. (9). С. 140-144.

Illia Kovalenko. Certain types of examinations as obligatory investigative (search) actions in the investigation of fraud in the field of bank electronic payments

The article covers the issues of research of types of computer-technical examinations, which are obligatory investigative (search) actions in the investigation of crimes involving the latest technologies and computer systems, such as fraud in the field of electronic bank payments. It also emphasizes that in order to better detect such complex criminal offenses, the knowledge base of experts and their methodological support must be constantly updated and ahead, because every second new technologies appear in the world and hundreds of thousands of US dollars are stolen every day. The most common hardware, devices and software that need to be examined by an expert in the framework of forensic computer and technical examination are considered. The sequence of actions of the expert at research of computer engineering for revealing of traces of criminal offenses is offered, and also opinions of the modern scientists who have studied this question are analyzed. It is proposed to divide the examination of the equipment used to commit fraud into four stages according to the types of forensic computer and technical examination, namely to begin research to identify hardware, then installed software, identify information, and finally identify network traces of attackers. Much attention has been paid to identifying the basic hardware that should be investigated by experts. The subject, tasks, and also actual questions concerning each of types of forensic computer and technical examination are defined. It was also stressed the importance of cooperation between state law enforcement agencies of Ukraine with international partners and experts in order to achieve the common goal of detecting fraud in the field of electronic bank payments, as well as the need for rapid communication between agencies of different countries. Emphasis is placed on the problem of competence of experts in the field of information technology and computer systems, logistics, as well as outdated software during forensic computer examination.

Key words: forensic computer technical expertise, internet banking, information technologies, traces of crime, cybercrime.