УДК 343.98:343.131 **DOI:** https://doi.org/10.32631/v.2024.2.15

Михайло Васильович Лепей,
кандидат юридичних наук,
Комунальне унітарне підприємство
«ЕкоВін» (заступник директора з юридичних питань);
https://orcid.org/0009-0005-9425-2923,
e-mail: lepei1991rada@gmail.com

НАУКОВІ ДИСКУСІЇ ЩОДО ПРОВЕДЕННЯ РІЗНИХ ВИДІВ ОГЛЯДУ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ ВИКОРИСТАННЯ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Статтю присвячено розгляду деяких аспектів розслідування шахрайства у сфері використання банківських електронних платежів. Проаналізовано особливості проведення різних видів огляду у кримінальних провадженнях визначеної категорії. Зазначено, що під час розслідування шахрайства у сфері використання банківських електронних платежів огляд місця події не втрачає свого значення, адже в багатьох випадках залишаються певні матеріальні сліди на місці вчинення протиправного діяння та в електронно-обчислювальній техніці, яка використовувалась для його вчинення. На основі вивчення матеріалів кримінальних проваджень зазначено, що до об'єктів, які необхідно досліджувати під час проведення огляду місця події, належать приміщення, де вчинялись шахрайські дії, інші місця, де вчинялись шахрайські дії, смартфон шахрая, паперові носії даних.

Ключові слова: кримінальні правопорушення, шахрайство, банківські електронні платежі, розслідування, кримінальне провадження, слідчі (розшукові) дії, огляд, електронно-обчислювальна техніка, потерпілий.

Оглядова стаття

Постановка проблеми

Огляд є першочерговою слідчою (розшуковою) дією в переважній більшості кримінальних проваджень, адже його проведення вирішує завдання початкового етапу розслідування щодо збору матеріальної доказової інформації вчиненого кримінального правопорушення. Під час розслідування шахрайства у сфері використання банківських електронних платежів зазначена процесуальна дія не втрачає свого значення. Це пояснюється тим, що в багатьох випадках залишаються матеріальні сліди на місці вчинення протиправного діяння та в електронно-обчислювальній техніці, яка використовувалась для його вчинення. Тому опрацювання обраної тематики сьогодні є доволі актуальним питанням як із доктринальної, так і з практичної точок зору.

Мета і завдання дослідження

Метою статті є дослідження особливостей проведення різних видів огляду під час розслідування шахрайства у сфері використання банківських електронних платежів. У межах визначеної мети потребують вирішення такі *завдання*: 1) проаналізувати особливості проведення різних видів огляду під час розслідування шахрайства у сфері використання банківських електронних платежів; 2) визначити особливості огляду місця події у кримінальних провадженнях вказаної категорії; 3) виокремити об'єкти, які необхідно досліджувати під час проведення огляду місця події.

Стан дослідження проблеми

Проблематиці проведення слідчих (розшукових) дій у різних категоріях кримінальних проваджень присвятили свої праці такі дослідники, як В. П. Бахін, А. Ф. Волобуєв, В. А. Журавель, А. В. Іщенко, В. Г. Лукашевич, Є. Д. Лук'янчиков, М. А. Погорецький, М. В. Салтевський, Р. Л. Степанюк, К. О. Чаплинський, С. С. Чернявський, Ю. М. Чорноус, В. Ю. Шепітько та ін. Крім того, аналізу проведення слідчих (розшукових) дій під час розслідування шахрайства у сфері використання банківських електронних платежів приділили увагу у своїх роботах такі науковці, як Б. М. Головкін, М. М. Єфімов, В. Б. Коба, І. О. Коваленко, О. Л. Мусієнко, Н. В. Павлова, А. В. Рейнгольд, О. А. Самойленко, С. В. Самойлов, К. О. Чередник, С. С. Чернявський, С. В. Чучко та ін. Водночас у межах нашого дослідження більш точно охарактеризовано різні аспекти окресленої процесуальної дії крізь призму сучасної судово-слідчої практики та позицій інших науковців.

Наукова новизна дослідження

У статті зроблено спробу опрацювати особливості проведення різних видів огляду під час розслідування шахрайства у сфері використання банківських електронних платежів, де особливу увагу приділено огляду місця події та електронно-обчислювальної техніки.

Виклад основного матеріалу

Вбачаємо доволі доречним твердження В. В. Сисолятіна, який зауважив, що «на початковому етапі розслідування є досить багато слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій, а також розшукових заходів, які варто провести в будь-якому випадку. Звісно, корелюючи їх у відповідності до конкретного протиправного діяння, яке було вчинено. Зокрема, під час розслідування вбивства – це огляд трупа та його експертиза для встановлення обставин та механізму смерті особи; крадіжки – огляд місця події для з'ясування механізму вчинення протиправного діяння та виявлення матеріальної доказової інформації; шахрайства – допит

потерпілого для визначення способу його вчинення тощо. Під час розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, безумовно також наявні обов'язкові процесуальні дії, які необхідно реалізувати до внесення відомостей в ЄРДР та одразу після цього для забезпечення належної доказової бази» [1, с. 129]. Отже, ми вважаємо обов'язковими слідчими (розшуковими) діями початкового етапу розслідування шахрайства у сфері використання банківських електронних платежів огляд місця події та огляд електронно-обчислювальної техніки.

Відповідно до частин 1 та 2 ст. 237 Кримінального процесуального кодексу України (далі – КПК України) з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та комп'ютерних даних. Огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі)[1]. А вже в ч. 3 ст. 214 КПК України вказано, що в невідкладних випадках до внесення відомостей до Єдиного реєстру досудових розслідувань може бути проведений огляд місця події (відомості вносяться невідкладно після завершення огляду)[2].

А. І. Кунтій, зі свого боку, зазначав, що «організація та технологія проведення огляду в справах про "комп'ютерні" злочини відрізняються від аналогічної слідчої (розшукової) дії під час розслідування традиційних злочинів. Це обумовлено не тільки небезпекою навмисного знищення інформації, яка має доказове значення, з боку ще не виявлених учасників злочину, інших зацікавлених осіб, але і необережним поводженням слідчого й інших членів слідчо-оперативної групи, які можуть зашкодити інформації, знищити сліди внаслідок неправильного, некваліфікованого поводження з програмно-апаратними засобами. Однією з найважливіших умов проведення огляду є суворе дотримання встановлених правил поводження з комп'ютерною технікою та носіями інформації, технічно грамотне проведення пошуку доказів, потрібної інформації. Також рекомендується обов'язково залучати до огляду спеціаліста в галузі інформатики та обчислювальної техніки. Нагадаємо, що лише огляд місця події у

[1] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 17.05.2024).

[2] Там само.

виняткових випадках, може бути проведений до внесення відомостей про кримінальне правопорушення до ЄРДР і після завершення такого огляду, слідчий, прокурор зобов'язаний негайно внести такі відомості до ЄРДР. Саме ця слідча (розшукова) дія сприяє вирішенню низки важливих питань, а саме:

– на якому об'єкті (на якому конкретно комп'ютері, у якому структурному підрозділі установи) сталася подія;

– до якого виду можна віднести комп'ютерний злочин, що відбувся;

– яким способом учинено злочин;

– які сліди чи інші речові докази вказують на причетність до злочину певної особи;

– яким є під час огляду стан засобів захисту інформації, охорони приміщень, обладнання та низка інших питань» [2, с. 879–880].

Вельми точною вбачаємо думку В. А. Журавля, який зауважує, що «законодавцем передбачено складну процедуру набуття об'єктами, вилученими з місця огляду події, статусу речових доказів, що не сприяє оперативності проведення досудового розслідування й економії процесуальних засобів. Мається на увазі те, що ці об'єкти спочатку визнаються як тимчасово вилучені (ст. 237 КПК України), далі слідчий протягом 24 годин повинен звернутися з клопотанням до слідчого судді про накладання арешту на ці тимчасово вилучені об'єкти (ст. 167 КПК України), і лише після прийняття відповідної ухвали слідчим суддею вони набувають статусу речових доказів» [3, с. 254]. Водночас вчений зазначає, що «відповідно до положень КПК 1960 року такого роду об'єкти набували статусу речових доказів одразу ж після їх належного оформлення в протоколі слідчого огляду та вилучення. Особливо складно здійснити зазначену процедуру в ситуації затримання особи в порядку статей 207, 208 КПК України, коли за добу треба встигнути оглянути місце події, відкрити кримінальне провадження, повідомити затриманому про підозру, процесуально правильно оформити вилучені з місця огляду об'єкти, звернувшись для цього до слідчого судді з відповідним клопотанням. Коли та як це зробити, залишається незрозумілим» [3, с. 254].

Для початку розглянемо особливості проведення огляду місця події. Зокрема, Є. І. Макаренко зазначив, що «огляд місця події – це невідкладна слідча дія, спрямована на безпосереднє встановлення, сприйняття, дослідження та фіксацію обстановки місця події (стану, властивостей і ознак матеріальних об'єктів, що перебувають на місці події), слідів злочину й інших фактичних даних, які в сукупності дозволяють зробити ґрунтовний висновок щодо характеру, механізму та мотивів злочину, особи злочинця й інших обставин, які підлягають доказуванню у разі порушення в подальшому кримінальної справи та провадження дізнання чи досудового слідства» [4, с. 12].

Щодо об'єктів огляду місця події вважаємо слушною думку А. В. Реуцького, який серед них виокремив приміщення: «(а) де обслуговуються розрахунки платіжними картками; (б) де знаходиться банкомат; (в) банківських установ або процесингових центрів; (г) де виготовлялися підроблені платіжні картки; (д) де встановлена комп'ютерна техніка, за допомогою якої вчинено злочин, або де знаходиться провайдер, що надає послуги доступу в мережу Інтернет; а також (е) ділянки території, по яких проходять кабелі зв'язку між учасниками системи, які обслуговують обіг платіжних карток, та ін.» [5, с. 126].

Л. П. Паламарчук вказує на те, що «матеріальні сліди також можуть залишатися на обчислювальній техніці (сліди від пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо), а також на магнітних носіях і оптичних дисках. До окремого типу належать інформаційні сліди, що утворюються внаслідок впливу на комп'ютерну інформацію (шляхом знищення, перекручення). Вони залишаються на магнітних носіях інформації та пов'язані зі змінами, які відбулися в самій інформації, порівняно з початковим її станом. Також до інформаційних слідів належать наслідки роботи антивірусних і тестових програм, які можуть бути виявлені під час вивчення комп'ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм і програмного забезпечення. Для виявлення подібних слідів необхідно залучати спеціаліста з комп'ютерної техніки та програмного забезпечення» [6, с. 8]. Зі свого боку В. І. Пазиніч вирізняє дві групи типових об'єктів огляду, як-от: «приміщення, автотранспорт та інші місця, де здійснювалося зберігання, клонування мобільних телефонів, виробництво інших радіоелектронних пристроїв, підробка документів; предмети, пов'язані зі вчиненням злочинів у сфері мобільних телекомунікацій: мобільний телефон злочинця, інші радіоелектронні пристрої, засоби комп'ютерної техніки злочинця і оператора мобільного зв'язку, паперові носії інформації» [7, с. 28].

На основі вивчення матеріалів кримінальних проваджень серед об'єктів, які необхідно досліджувати під час проведення огляду місця події, нами було виокремлено такі: приміщення, де вчинялись шахрайські дії, інші місця, де вчинялись шахрайські дії, смартфон шахрая, паперові носії даних.

Щодо огляду електронно-обчислювальної техніки, то, наприклад, П. Д. Біленчук, Д. П. Біленчук, В. Б. Міщенко й О. І. Мотлях зауважують, що «огляд комп'ютерної техніки дозволяє з'ясувати ряд відомостей про способи скоєння шахраєм протиправної дії, їх вірогідні мотиви та мету. В окремих випадках бажано, щоб підозрюваний був присутній при огляді його комп'ютера, оскільки саме він може надати найважливішу інформацію про особливості функціонування

комп'ютерної системи, зокрема таку, як: 1) паролі, коди доступу; 2) перелік інстальованих комп'ютерних програм (програм, які є у комп'ютері); 3) місцезнаходження окремої інформації на машинному носії (окремих директорій, у тому числі прихованих)» [8, с. 66–67]. Тобто основними моментами при проведенні огляду електронно-обчислювальної техніки буде з'ясування паролів та кодів доступу, а також встановлення місцезнаходження конкретних відомостей на машинному носії.

О. М. Юдін, М. В. Макарова та Р. М. Лавренюк засвідчили, що «при огляді веб-сторінки сайту, слід враховувати наступні моменти. Так, необхідно, щоб на сайті були витримані:

– єдині стандарти фірмового стилю (єдина символіка, кольорова гама, прийоми верстки, фірмові персонажі);

– грамотна манера написання текстів, їх характер (єдиний стиль, жанр);

– корпоративні стандарти обслуговування клієнтів (дотримання ціннісних орієнтирів, певної манери спілкування, швидкість реагування, обрання пріоритетів). Усі перераховані інструменти брендингу повинні підсилювати один одного, тим самим створюючи загальний образ компанії, підтримуваний сайтом. При адаптації фірмового стилю до застосування на Web-сайті:

– логотип компанії має розташовуватися нагорі усіх сторінок, не повинен бути викривлений або зіпсований;

– навколо логотипа мають бути залишені стандартні поля (так звана «захисна зона», розміри якої зазвичай пропорційні самому логотипу);

– слоган компанії повинен розташовуватися в помітному місці й відтворюватися абсолютно точно;

– якщо в компанії є фірмовий персонаж, то його зображення може бути присутнім на сайті;

– при підборі ілюстрацій необхідно дотримуватися іміджевої політики компанії (наприклад, використовувати певні фотографії, піктограми, іконки);

– на сайт можуть бути в адаптованому вигляді перенесені деякі прийоми форматування тексту, характерні для фірмової поліграфії (наприклад, способи оформлення заголовків, цитат, виносок тощо);

– невелике зображення, що виводиться в адресний рядок браузера (англ. – favicon, скор. від англ. FAVorites ICON – "значок для обраного"), повинно бути намальовано з урахуванням фірмової символіки компанії і повторювати її фірмовий знак» [9, с. 44].

Доволі слушною вважаємо позицію Д. А. Птушкіна, який наголошував на тому, що «шахраї нерідко використовують комп'ютерну техніку для підготовки проєктів різних підроблених документів,

зберігання відео- або фотофайлів, ведення переговорів у мережі Інтернет і електронною поштою, відвідування соціальних мереж. У пам'яті комп'ютера можуть бути адреси потенційних жертв, графічні зразки бланків тощо. Крім того, на флеш-карті мобільного телефону також може зберігатися значна кількість інформації про контакти, зв'язки тощо. Тому така інформація, безсумнівно, становить інтерес для слідства та спрямовує правоохоронні органи в правильному напрямку» [10, с. 79].

І. О. Коваленко вказує на те, що варто звертати увагу на «специфіку об'єктів, які оглядаються. При огляді треба залучати відповідних ІТ-фахівців з кібербезпеки із залученням спеціальних технічних засобів для виявлення, встановлення та вилучення певної інформації, яка знаходиться на електронних носіях та слугуватиме доказами по даному кримінальному правопорушенню. Адже місце події для уповноваженої особи носить дослідницький характер, спрямований на встановлення обстановки події, виявлення слідів протиправного діяння та з'ясування інших обставин, які можуть пришвидшити його розкриття» [11, с. 125]. Як бачимо, залучення ІТ-фахівців для проведення огляду електронно-обчислювальної техніки є обов'язковим заходом під час здійснення процесуальних дій.

Висновки

Підбиваючи підсумок, зауважимо, що обов'язковими слідчими (розшуковими) діями початкового етапу розслідування шахрайства у сфері використання банківських електронних платежів є огляд місця події та огляд електронно-обчислювальної техніки. На основі вивчення матеріалів кримінальних проваджень серед об'єктів, які необхідно досліджувати під час проведення огляду місця події, виокремлено такі: приміщення, де вчинялись шахрайські дії; інші місця, де вчинялись шахрайські дії; смартфон шахрая; паперові носії даних. Визначено, що основними моментами при проведенні огляду електронно-обчислювальної техніки буде з'ясування паролів та кодів доступу, а також встановлення місцезнаходження конкретних відомостей на машинному носії. З'ясовано, що залучення ІТ-фахівців для проведення огляду електронно-обчислювальної техніки є обов'язковим заходом під час здійснення окреслених процесуальних дій.

Список бібліографічних посилань: 1. Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09. Київ, 2024. 232 с. **2.** Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., перероб. та допов. Львів : ЛьвДУВС, 2016. 948 с. **3**. Журавель В. А. Початок досудового розслідування: деякі процесуальні та організаційно-тактичні проблеми. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2015. № 1. С. 251–258. **4.** Макаренко Є. І.

Огляд місця події: довідник дільничного інспектора міліції. Дніпропетровськ : Юрид. акад. МВС, 2004. 210 с. **5.** Реуцький А. В. Методика розслідування злочинів у сфері иготовлення та обігу платіжних карток : дис. … канд. юрид. наук : 12.00.09. Харків, 2009. 198 с. **6.** 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. Київ, 2005. 21 с. **7.** Пазиніч В. І. Особливості порушення кримінальної справи і початкового етапу розслідування злочинів, які пов'язані з втручанням в роботу мереж мобільного зв'язку. *Іменем Закону.* 2007. № 2. С. 27–29. **8.** Біленчук П. Д., Біленчук Д. П., Міщенко В. Б., Мотлях О. І. Національна безпека України: сучасні інформаційні технології і можливі джерела безпеки. *Вісник Академії праці і соціальних відносин ФП України.* 1998. № 1. С. 61–72. **9.** Юдін О. М., Макарова М. В., Лавренюк Р. М. Системи електронної комерції: створення, просунення і розвиток : монографія. Полтава : РВВ ПУЕТ, 2011. 201 с. **10.** Птушкін Д. А. Розслідування шахрайства, вчиненого щодо об'єктів нерухомого майна громадян : дис. … канд. юрид. наук : 12.00.09. Дніпро, 2018. 240 с. **11.** Коваленко І. О. Деякі аспекти проведення огляду місця події при розслідуванні шахрайства у сфері використання банківських електронних платежів // Актуальні проблеми забезпечення публічного порядку та безпеки в сучасних умовах: вітчизняний та міжнародний досвід : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 25 жовт. 2019 р.) / МВС України, Дніпропетровськ. держ. ун-т внутр. справ. Дніпро, 2019. С. 123–125.

Надійшла до редколегії 20.05.2024

Прийнята до опублікування 16.06.2024

Lepei M. V. Scientific discussions on conducting different types of examination during the investigation of fraud in the field of electronic payments

The article is devoted to consideration of some aspects of investigation of fraud in the sphere of electronic payments. The author analyses the peculiarities of conducting various types of examination in criminal proceedings of this category.

It is noted that inspection is the primary investigative (detective) action in the vast majority of criminal proceedings, since it solves the task of the initial stage of investigation to collect material evidentiary information of a criminal offence. In the course of investigation of fraud in the field of electronic payments, this procedural action does not lose its importance, since in many cases certain material traces remains at the place of commission of the unlawful act and in the electronic computing equipment used to commit it.

It is also emphasised that the mandatory investigative (detective) actions at the initial stage of investigation of fraud in the field of electronic payments are inspection of the scene and inspection of electronic computing equipment.

Based on the study of criminal proceedings, the article indicates that the objects to be examined during the inspection of the scene include the premises where the fraudulent acts were committed, other places where fraudulent acts were committed, the fraudster's smartphone, and paper data carriers.

It is determined that the main points in the inspection of electronic computing equipment are to find out passwords and access codes, as well as to establish specific information on the machine media. It is found that the involvement of IT specialists in the inspection of electronic computing equipment is a mandatory measure in the course of procedural actions.

Key words: criminal offences, fraud, bank electronic payments, investigation, criminal proceedings, investigative (search) actions, inspection, electronic computing equipment, victim.