УДК: 343.98
ORCID: 0000-0003-1861-8354
e-mail: gull_ukr@ukr.net

Larysa P. Grynko,
‘ at the Department of Criminal Law and Criminal Law Disciplines
(Poltava Law Institute of TheYaroslav Mudryi National Law University)

Гринько Лариса Петрівна,
доцент кафедри кримінального права та кримінально-правових дисциплін
(Полтавський юридичний інститут Національного юридичного університету імені Ярослава Мудрого)

«СЛІДОВА КАРТИНА» ШАХРАЙСТВ ВЧИНЕНИХ ЧЕРЕХ МЕРЕЖУ ІНТЕРНЕТ

«TRACE PICTURE» OF FRAUD ON THE INTERNET

Анотація. У статті надано характеристику слідової картини шахрайств, учинених через мережу Інтернет. Проаналізовано судову практику та позиції вчених-криміналістів з окресленої проблематики, зокрема на основі аналізу судової практики узагальнено статистичні дані. За результатами проведеного дослідження проаналізовано сліди, які залишають злочинці при вчинення шахрайств в мережі Інтернет (віртуальні та матеріальні). Наголошено, що крім матеріальних та ідеальних слідів, особливе місце посідають віртуальні сліди злочину, що як наслідок, суттєво впливають на його розкриття та розслідування. Досліджуваний злочин характеризується високою латентністю, насамперед, через складнощі виявлення слідів такого злочину. Тому, особливу увагу приділено дослідженню віртуальних слідів. Запропоновано поділ віртуальних слідів на сліди, які залишаються на електронних носіях та ті, які містяться в мережі Інтернет. Це сліди, які залишаються на сторінках соціальних мереж; рахунках в електронних платіжних засобах та системах; серверах електронних пристроїв; серверах мобільного оператора; інтернет-сайтах; URL Веб сторінках; на накопичувачах пам’яті електронних пристроїв. Матеріальні слідів знаходять

свій прояв у вигляді: слідів пальців рук, що залишаються на мобільних пристроях, планшетах, комп'ютерах та носіях, що використовувались під час вчинення шахрайства, а також предметах, отриманих у його результаті; роздруківки файлів, переписки, скринів, фотозображень з комп'ютерних та інших електронних пристроях; роздруківки банківських рахунків; квитанцій, чеки про оплату, платіжні доручення тощо. Специфічність слідів шахрайств, вчинених через мережу Інтернет зумовлює труднощі у виявленні та розслідуванні зазначеної категорії злочинів. Такий стан потребує належного їх аналізу та дослідження, що реалізує можливість розробки методичних рекомендації для подальшого розслідування та розкриття цього різновиду кримінальних правопорушень.

Ключові слова: шахрайство, комп'ютерні технології, шахрайство в мережі Інтернет, кіберзлочини, слідова картина шахрайств, віртуальні сліди, кіберпростір.

Summary. The article describes the trace pattern of fraud committed through the Internet. Analyzed the judicial practice and the positions of forensic scientists on the outlined issues. Based on the results of the research, traces left by criminals when committing fraud on the Internet were analyzed. It is emphasized that in addition to material and ideal traces, a special place is occupied by virtual traces of a crime, which, as a result, significantly affects the complexity of its disclosure and investigation. The investigated crime is characterized by high latency, primarily due to the difficulty of detecting traces of such a crime. Therefore, special attention is paid to the study of virtual traces. The division of virtual traces into traces that remain on electronic media and those contained in the Internet is proposed. These are traces that remain on the pages of social networks; accounts in electronic means of payment and systems; servers of electronic devices; mobile operator servers; Internet sites; URL of web pages; on memory drives of electronic devices. Material traces are manifested in the form of: fingerprints left on mobile devices, tablets, computers and media used during fraud, as

well as items obtained as a result of it; printouts of files, correspondence, screens, photos from computer and other electronic devices; printouts of bank accounts; receipts, payment checks, payment orders, etc. The specificity of traces of fraud committed through the Internet causes difficulties in detecting and investigating the specified category of crimes. Such a state requires their proper analysis and research, which will provide an opportunity to develop methodological recommendations for further investigation and disclosure of this type of criminal offenses.

Keywords: fraud, computer technology, fraud on the Internet, cybercrime, fraud pattern, virtual traces, cyberspace.

Постановка проблеми. Впровадження нових технологій безпосередньо корелює з зростанням числа користувачів мережею Інтернет, що, безумовно, впливає і на підвищення рівня кіберзлочинності. За останні п’ять років в Україні кількість інформаційних злочинів зросла щонайменше у 2,5 рази [1]. Пандемія коронавірусу змусила людство все більше переходити в інформаційний простір, що також вплинуло на зростання кіберзлочинів на 25% [2].

Серед злочинів, що вчинюються в мережі Інтернет, особливе місце займають шахрайства. Інтернет-шахрайства характеризуються високим рівнем латентності, що зумовлено бурхливим розвитком інформаційних технологій та запровадженням нових способів вчинення цього злочину. Нині шахрайство з використанням можливостей мережі «Інтернет», як вважає С.В. Шапочка, зберігає сталу тенденцію до еволюціонування, з’являються нові його види чи вдосконалюються вже відомі, зокрема: у сфері дистанційного банківського обслуговування, з електронними платіжними системами й 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»), застосування шпигунських програм (spyware,

keyloggers), використання програмного забезпечення, sms-шахрайство тощо [3, с. 145]. Такий стан зумовлює дослідження та розробку нових методів протидії злочинності.

Стан опрацювання обраної проблематики, аналіз останніх публікацій та досліджень. Слідова картина шахрайств, вчинених через мережу Інтернет, була предметом досліджень багатьох науковців. Зокрема, присвятили свої праці А. І. Анапольська, Р. С. Атаманов, Н. М. Ахтирська, А. Ф. Волобуєв, С. В. Головкін, С. М. Князєв, Н. Ю. Кириленко, С. М. Князєв, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, В. П. Сабадаш, С.В. Самойлов, М. М. Федотов, С. С. Чернявський, С. В. Шапочка, А. Ю. Юрчук та інші. Разом з тим, стрімкий розвиток сучасних інформаційних технологій надав можливість зародження нових способів злочинних діянь, що стало негативним явищем та вимагає сучасних методів дослідження, розкриття та розслідування шахрайств, вчинених через мережу Інтернет і є одним з актуальних питань, яке постає сьогодні.

Метою статті є надання характеристики слідової картини шахрайств, вчинених через мережу Інтернет як елемента криміналістичної характеристики розглядуваного виду злочину.

Виклад основного матеріалу. Будь-який злочин змінює первинну обстановку. Виявлення та аналіз таких змін, зокрема наявних слідів злочину, має важливе значення для всебічного, повного та об’єктивного дослідження усіх обставин злочинної події.

Слідова картина злочину - це сукупність джерел матеріальних та ідеальних відображень у навколишній матеріальній обстановці вчиненого злочину [4, с. 253]. Матеріальні сліди злочину включають у себе сліди-відображення, сліди-предмети і сліди-речовини. Ідеальні сліди злочину – це уявний образ у пам’яті особи, що відображає подію в свідомості людини.

У разі вчинення шахрайств через мережу Інтернет, їх сліди мають істотні особливості, пов’язані з тим, що вчинення злочину здебільшого пов’язане з

використанням великого різноманіття носіїв комп'ютерної інформації, що мають різну природу – пам'ять комп'ютера, лінії електрозв'язку, роздруківки матеріалів із принтера тощо, для роботи з якими потрібні різноманітні технічні засоби, а в багатьох випадках – ще й навички та спеціальні знання [5, с. 5]. Тому, слід погодитись з авторами, які наголошують, що сліди комп'ютерних злочинів рідко виявляються у змінах навколишнього середовища [6, с. 38; 7, с. 263]. Такі сліди, по більшій мірі, утворюються в інформаційному просторі та відбиваються на апаратних, програмних чи інформаційних елементах носіїв комп'ютерної інформації. Звичайно, виникають складнощі як зі встановленням тих користувачів, які безпосередньо вчиняють шахрайські дії, так і встановленням слідів, які залишили злочинці.

Це пояснюється тим, що віртуальний штучно створений простір, в якому моделюється, зберігається, переміщається інформація закодована, як правило, з використанням двійкового коду, яка може становити найрізноманітніші відомості про об'єктивний світ. Така інформація зберігається в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки й передачі, таких як жорсткі диски, кластери логічних дисків, сервери – data center, онлайн-сховища – cloud storage, внутрішні енергозалежні флеш-пам'яті, зовнішні карти пам'яті тощо [8, с. 5].

При вчиненні шахрайств через мережу Інтернет, у більшості випадків, злочинці використовують телефон, комп'ютер, ноутбук, планшет або інший пристрій, кожний з яких має свою IP-адресу, тобто адресу вузла, з якого можуть заходити користувачі, але за якою неможливо встановити конкретний унікальний комп'ютер, з якого здійснювалося шахрайство. Як пишуть В.М. Горлач та В.М. Макар, IP-адреса складається з адреси мережі, підмережі та локальної хост-адреси (Host), яка є унікальна для кожного вузла. Кожен хост може мати не тільки IP-адресу, але й ім'я, які діляться на частини, що розділяються крапками. Список таких імен зберігається в спеціальній базі даних доменів служби імен DNS (Domain Name System) [9, с. 21]. Виходячи з цього,

можна стверджувати, що одним із головних завдань є встановлення точок доступу, з яких здійснювалися шахрайські дії злочинця.

Розглядаючи віртуальні сліди, треба зазначити, що ці сліди несуть в собі значущу інформацію нарівні з традиційними видами слідів. Цієї думки дотримується ряд вчених. Так, В.О. Мещеряков виокремлює віртуальні сліди в самостійну групу нарівні з ідеальними та матеріальними. Він вважає, що в результаті електронно-цифрового відображення на матеріальному носії фіксується образ з цифрових значень параметрів формальної математичної моделі спостережуваного реального фізичного явища [10, с. 266]. Такої ж думки і Я. Найдьон, яка доповнює класифікацію слідів віртуальними та розглядає їх як цифровий образ, електронні сигнали, що залишаються в пам'яті електронних і подібних до них пристроїв, що передаються за допомогою заданого алгоритму і мають кримінально-релевантне значення. Віртуальні сліди можна розглядати як діяльність особистості у віртуальному просторі [11 с. 306].

Крім того, сутність віртуальних слідів проявляється у їх характерних ознаках, серед них: відсутність фізично цілісної структури; зв'язок із матеріальним носієм; специфічний механізм слідоутворення; багато компонентний характер, складна інформаційна структура, в якій поряд зі значущою кримінально-релевантною інформацією міститься значний обсяг допоміжних даних, що відповідають за цілісність і доступність комп'ютерної інформації віртуального сліду; вилучення віртуальних слідів можливе лише за допомогою спеціальних програмно-технічних засобів; нестабільний характер, адже вони не мають міцного зв'язку із записуючим інформацію пристроєм, а також легко піддаються знищенню [12 с. 378].

Щодо класифікації віртуальних слідів, то у криміналістичній літератури здійснювалися спроби виокремити віртуальні сліди. Так, Я. Найдьон поділяє віртуальні сліди на 4 групи: - за походженням: 1) електронна інформація, створена ЕОМ у процесі своєї роботи; 2) електронна інформація, створена в процесі діяльності людини; 3) похідна електронна інформація, створена

комп’ютером на основі введених даних користувачем, або навпаки, інформація, створена з даних, згенерованих комп’ютерною системою; - за формою подання: 1) людиночитабельна інформація (інформація, доступна для сприйняття людиною); 2) машиночитабельна інформація (інформація, представлена у вигляді машинного коду); -за місцем зберігання: 1) дані, що зберігаються в комп’ютерних системах (ЕОМ, сервери, локальні мережі, глобальні мережі); 2) дані, скопійовані або переміщені користувачем на електронні носії (жорсткі диски, компакт-диски, накопичувачі); 3) паперові копії людиночитабельної або машиночитабельної інформації (копії листування, скріншоти та ін.); - за формою: 1) вихідні дані (інформація, введена людиною); 2) людиночитабельні та машиночитабельні бази даних; 3) коди шифрування; 4) програмне забезпечення різних видів; 5) комп’ютерні системи (ЕОМ, сервери, локальні мережі, глобальні мережі) [11 с. 305-306].

А.Б. Смушкин вважає, що будь-які дії з високоточними пристроями залишають свій слід в їхній пам’яті. Найбільш явними у такому разі виступають сліди в пам’яті комп’ютера, які поділяються на сліди включення і виключення, а також сліди різних операцій із вмістом пам’яті, сліди дій з програмами і відомості про роботу в мережі Інтернет, локальних та інших мережах. Віртуальні сліди є доказами вчинення або планування злочину конкретною особою або групою осіб [13, с. 44].

О.Л. Мусієнко в основу класифікації покладає процесуальне положення суб’єкта: 1) сліди на комп’ютері злочинця; 2) сліди на комп’ютері жертви [14, с. 56].

Г.К. Авдєєва та С.В. Стороженко до видів електронних слідів включають :

- інформацію, яка міститься в журналах операційних систем та окремих програмних продуктів,

- дані електронного листування, за допомогою яких можна встановити дату та час, адресу відправника тощо,

- дані на різних сайтах (Facebook, Twitter), які залишають електронні сліди у вигляді повідомлень, пошукових запитів, фотознімків тощо [15, с. 171].

Аналіз судової практики по справам про шахрайства, вчинених через мережу Інтернет, свідчить, що віртуальні сліди є найбільш розповсюдженими і складають 67 % від загальної кількості узагальненої судової практики, на відміну від матеріальних й ідеальних, які в свою чергу складають лише 29% і 4%.

Віртуальні сліди можна поділити на сліди, які залишаються на електронних носіях та ті, які містяться в мережі Інтернет. Це сліди, які залишаються на:

- сторінках соціальних мереж («Instagram», «Фейсбук» та інші) у вигляді інформації про товар, переписки, прикріплених фото товару тощо (складає 74%). Так, ОСОБА_1 умисно з корисливих мотивів для власного безпідставного збагачення шляхом обману та зловживання довірою, шляхом незаконних операцій із використанням електронно-обчислювальної техніки для вчинення шахрайських дій, зловживаючи довірою потерпілої ОСОБА_2, ІНФОРМАЦІЯ_2, жительки АДРЕСА_2 , яка ґрунтувалася на довірливих відносинах, що склалися між ними внаслідок листування в соціальній мережі «Інстаграм», викликаних бажанням ОСОБА_2 придбати кросівки марки «UTERQUE», оголошення про продаж яких було оприлюднено в соціальній мережі «Інстаграм», за інтернет-посиланням ІНФОРМАЦІЯ_3 усвідомлюючи протиправний та суспільно небезпечний характер своїх дій та їх наслідків, заволоділа майном ОСОБА_2, а саме грошовими коштами в загальній сумі 3 690 грн. [16].
- рахунках в електронних платіжних засобах та системах (16%);
- серверах електронних пристроїв (IP-адреса комп’ютерного обладнання), що дозволяє встановити точку доступу до комп’ютера (67%);
- серверах мобільного оператора (43%). Прикладом є наступна справа. ОСОБА_1 , діючи умисно з корисливих мотивів для власного безпідставного збагачення, шляхом обману та зловживання довіри, шляхом незаконних операцій

із використанням електронно-обчислювальної техніки, а саме Інтернет-ресурсу, призначеного для розміщення повідомлень, з метою вчинення шахрайських дій, перебуваючи на території Шевченківського району м. Львова, у невстановленому досудовому розслідуванні точному місці в кінці 2021 року створила сторінку в соціальній мережі «Фейсбук» під назвою « ОСОБА_7 », за допомогою якої розмістила оголошення про надання послуг по оренді житла в групі соціальної мережі «Фейсбук», з вказанням мобільного номеру телефону НОМЕР_1 . В подальшому, ОСОБА_1 , використовуючи мобільний номер телефону НОМЕР_1 , з зареєстрованим на ньому месенджером «Вайбер», 08.03.2022 за допомогою телефонних дзвінків та шляхом надсилання текстових повідомлень, запропонувала та обговорила з потерпілим ОСОБА_2 умови оплати та надання послуг по оренді житла за адресою: АДРЕСА_2 , яким не володіла та не мала на меті здавати в оренду [17];

- інтернет-сайтах, у вигляді фотографій, відгуків та коментарій, результатів спілкування злочинця і потерпілого) (33%);
- URL Веб сторінках (7 %);
- накопичувачах пам’яті електронних пристроїв, за допомогою яких передається інформація (жорсткі диски, магнітні стрічки, оптичний диск, дискета, пам’ять телефону, пам'ять сім карт, пам'ять флеш карт), у вигляді електронних документів, слідів з’єднання, історії інтернет-браузера, sms повідомлення, фото, скрин переписки, історії голосових повідомлень тощо (54%).

До матеріальні слідів можна віднести сліди у вигляді:

- слідів пальців рук, що залишаються на мобільних пристроях, планшетах, комп’ютерах та носіях, що використовувались під час вчинення шахрайства, а також предметах, отриманих у його результаті (6%);
- роздруківки файлів, переписки, скринів, фотозображень з комп’ютерних та інших електронних пристроях (38%);
- роздруківки банківських рахунків (34%);

- квитанцій, чеки про оплату, платіжні доручення (22%) тощо.

Основою вчинення шахрайства є вміння злочинця грати на почуттях людей, використовувати слабкі сторони їх характеру, маніпулювати їх діями. Тому типовими слідами шахрайства є сліди, які залишилися у свідомості потерпілого, його близького оточення, свідків. Залежно від суб'єктивних можливостей потерпілого, часу контакту з шахраєм, жертва може до дрібниць описати зовнішність шахрая (шахраїв), його поведінку, особливі прикмети міміки, голосу, ходи, наявність згубних звичок, прикмети одягу. Важливого значення набуває повідомлення потерпілим змісту розмови із злочинцем, обізнаності останнього у особливостях певної сфери життєдіяльності, у якій шахрай проявив себе спеціалістом [18, с. 54].

Висновки та пропозиції. Бурхливий розвиток інформаційних технологій породжує нові способи вчинення Інтернет-шахрайств. Багатоманіття способів шахрайства зумовлює широкий спектр слідів його вчинення. Специфічність слідів шахрайств, вчинених через мережу Інтернет, створює труднощі у виявленні та розслідуванні зазначеної категорії злочинів. Такий стан потребує належного їх аналізу та дослідження, що надасть можливість розробки методичних рекомендації для подальшого розслідування та розкриття цього різновиду кримінальних правопорушень.

ЛІТЕРАТУРА

1. 1. За п'ять років кіберзлочинність в Україні виросла вдвічі. *Економічна правда.* 2021. URL: https://www.epravda.com.ua/news/2019/10/21/652782/. (дата звернення: 06.09.2022).

2. Кількість кіберзлочинів в Україні в 2021 році зросла на 25%. *РБК-Україна*. 2021. URL: https://www.rbc.ua/ukr/news/kolichestvo-kiberprestupleniy-ukraine-2021-1622012394.html. (дата звернення: 06.09.2022).

3. Шапочка С.В. До питання запобігання окремим видам шахрайства, яке вчинюється з використанням можливостей мережі Інтернет. *Боротьба з*

організованою злочинністю і корупцією (теорія і практика). 2014. № 1 С. 145-149.

4. Кузьмічов В. С. Криміналістика : навч. посіб. Київ: Юрінком Інтер, 2001. 368 с.

5. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. ... канд. юрид. наук. Київ. 2008. 20 с.

6. Паламарчук Л. П. Розслідування злочинів у сфері використання комп'ютерних технологій : монографія. Київ, 2007. 144 с.

7. Дуда Х. І. Поняття комп'ютерних слідів злочину. *Науковий вісник Національного університету біоресурсів і природокористування України.* 2014. №197 (Ч. 1). С. 262-267.

8. Майстренко М.М., Татарин І.І. Проблемні аспекти доказування шахрайств, вчинених у кіберпросторі. *Науковий вісник міжнародного гуманітарного університету. Сер. : Юриспруденція*. 2021. № 52. С. 85-89.

9. Горлач В.М., Макар В.М. Побудова та адміністрування INTRANET-мереж. Ч. 1. Основи мережних технологій : Тексти лекцій. Львів, 1999. 45 с.

10. Мещеряков В.А. Следы преступлений в сфере высоких технологий *Библиотека криминалиста.* 2013. № 5 (10). С. 265-269.

11. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019 № 5. С. 304-307. URL: http://pgp-journal.kiev.ua/archive/2019/5/57.pdf. (дата звернення: 06.09.2022).

12. Хижняк Є.С. До питання визначення поняття «віртуальні сліди». URL: http://dspace.onua.edu.ua/bitstream/handle/11300/15070/Хижняк%pdf.(дата звернення: 06.09.2022).

13. Смушкин А.Б. Виртуальные следы в криминалистике. *Законность.* 2012. № 8. С. 43-45.

14. Мусієнко О.Л. Теоретичні засади розслідування шахрайства в сучасних умовах: монографія. Харків: Право, 2009. 168 с. URL:

https://library.nlu.edu.ua/POLN_TEXT/MONOGRAFII_2010/Musienko_2009.pdf. (дата звернення: 09.09.2022).

15. Авдєєва Г.К., Стороженко С.В. Електронні сліди: поняття та види. URL: http://dspace.nlu.edu.ua/bitstream/123456789/13283/1/ (дата звернення: 09.09.2022).

16. Вирок Коломийського міськрайонного суду Івано-Франківської області від 25.03.2022 року, справа № 346/5233/21. URL: https://reyestr.court.gov.ua/Review/103771378. (дата звернення: 09.09.2022).

17. Вирок Шевченківського районного суду м. Львова від 22.07.2022 року, справа № 466/2568/22 https://reyestr.court.gov.ua/Review/105375720. (дата звернення: 09.09.2022).

18. Головкін С.В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування: дис. ... канд. юрид. наук. Луганськ. 2008. 216 с.