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

Larysa P. Grynko,
Associated Professor of 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)

ФІШИНГ ЯК СПОСІБ ВЧИНЕННЯ ШАХРАЙСТВА У МЕРЕЖІ ІНТЕРНЕТ

PHISHING AS A METHOD OF COMMITTING FRAUD ON THE INTERNET

Анотація. В статті розглядається сучасний стан та окремі криміналістичні аспекти протидії такому виду інтернет-шахрайству як фішингу. Досліджуються статистичні дані щодо таких злочинних проявів в Україні та світі. Автором вказуються способи інтернет-шахрайства, види фішингу та його характерні риси. Надано криміналістичну характеристику розслідування шахрайств, учинених з використанням комп'ютерних технологій (способу вчинення злочину, місце, предмет злочину тощо). Обґрунтовано підхід до поділу способів учинення шахрайств, учинених з використанням комп'ютерних технологій. Проаналізовано обстановку, час та місце вчинення досліджуваного злочину. Виокремлено окремі слідчі дії, які на першочерговому етапі займають суттєве місце в системі збирання доказів при розслідуванні шахрайств, учинених з використанням комп'ютерних технологій. Надані рекомендації щодо використання спеціальних знань під час розслідування шахрайств, учинених з використанням комп'ютерних технологій, зокрема, проведення ряду судових експертиз. Проаналізовано судову практику та позиції вчених-криміналістів з

окресленої проблематики. За результатами проведеного дослідження проаналізовано сліди, які залишають злочинці при вчинення фішингу в мережі Інтернет. Наголошено, що крім матеріальних та ідеальних слідів, особливе місце посідають цифрові сліди злочину, що як наслідок, суттєво впливають на його розкриття та розслідування. Досліджуваний злочин характеризується високою складністю через складнощі виявлення слідів такого злочину. Тому, особливу увагу приділено дослідженню цифрових слідів, видів експертиз та ін. Запропоновано поділ цифрових слідів на сліди, які залишаються на електронних носіях та ті, які містяться в мережі. Це сліди, які залишаються на 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 пристрояхТакий стан потребує належного їх аналізу та дослідження, що надасть можливість розробки методичних рекомендації для подальшого розслідування та розкриття цього різновиду кримінальних правопорушень.

Ключові слова: шахрайство, комп'ютерні технології, шахрайство в мережі Інтернет, кіберзлочини, фішинг, кіберпростір.

Summary. The article discusses the current state and specific forensic aspects of combating phishing as a form of internet fraud. Statistical data on such criminal manifestations in Ukraine and worldwide are examined. The author outlines the methods of internet fraud, types of phishing, and its characteristic features. The forensic characteristics of investigating fraud committed using computer technologies (method of crime, location, crime scene, etc.) are provided. An approach to categorizing methods of fraud committed using computer technologies is justified. The situation, timing, and location of the investigated crime are analyzed. Specific investigative actions that play a significant role in evidence gathering during the investigation of fraud committed using computer technologies are highlighted.

Recommendations are provided regarding the use of specialized knowledge in the investigation of fraud committed using computer technologies, including conducting a series of forensic examinations. Judicial practices and positions of forensic scientists on the outlined issues are analyzed. Based on the results of the study, traces left by criminals when committing phishing in the Internet are analyzed. It is emphasized that in addition to material and ideal traces, digital traces of the crime hold a special place, significantly impacting its detection and investigation. The investigated crime is characterized by a high level of complexity due to the difficulties in detecting traces of such crime. Therefore, particular attention is given to the examination and research of digital traces, categorizing them as traces left on electronic media and those found within the network. These include traces left on accounts in electronic payment instruments and systems, servers of electronic devices, mobile operator servers, websites, URL web pages, and storage devices of electronic devices. Material traces manifest themselves in the form of fingerprints left on devices. Such a state requires their proper analysis and research, which will provide the 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, phishing, cyberspace.

Постановка проблеми. Останнім часом все частіше особи стають заручниками кіберзлочинів. Високотехнологічні злочини набувають усе більш організованого та транснаціонального характеру. Серед злочинів, що вчинюються в мережі Інтернет, особливе місце займають шахрайства. Шахрайство пронизує усі сфери суспільного життя. Крім постачальників послуг, від дій кібершахраїв страждають клієнти банків, платіжних систем, користувачі телефонних мереж і Інтернет, сервісів електронної й мобільної комерції. Зростаючий збиток від дій зовнішніх і внутрішніх шахраїв створює погрозу

розвитку нових перспективних секторів ринку електронних послуг, гальмує впровадження інновацій в економіку й державне управління [1, с. 278].

Злочинці використовують різноманітні способи шахрайства через мережу Інтернет, де одним з найбільш розповсюджених є фішинг. Він є одним з найпоширеніших форм шахрайства, який використовують злочинці для привласнення коштів або отримання облікових даних. Лише у 2022 року експерти SlashNext зафіксували більше 255 млн. фішингових атак, що на 61% більше, ніж 2021 року. При цьому на 50% збільшились атаки на мобільні пристрої, на 80% збільшилися загрози від довірених служб, таких як Microsoft, Amazon Web Services або Google, при цьому майже третина (32%) усіх загроз наразі розміщуються на довірених сервісах, 54% всіх виявлених загроз були нульовим годинником, показуючи, як хакери змінюють тактику в режимі реального часу для підвищення успіху, 76% загроз були націлені на атаки фішингу на збір облікових даних [2].

В Україні у 2022 році спостерігалось суттєве збільшення його проявів. Найпоширенішим видом стала фейкова соціальна допомога від державних чи міжнародних організацій постраждалим від війни українцям. У 2022 році НБУ виявив близько 4500 фішингових ресурсів, для порівняння – в 2021 році ця цифра була на порядок меншою [3].

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України спільно з Національним банком України запустили проєкт із протидії кібершахрайству у фінансовому секторі. Головна його мета – посилити захист громадян від кіберзлочинців, які суттєво активізували діяльність у період воєнного стану в Україні. Для крадіжки коштів зловмисники проводять фішингові кампанії, метою яких є виманювання даних для доступу до банківських рахунків. Результати вражають: лише за перший місяць зафіксовано близько 120 тисяч унікальних переходів на сторінку з попередженням, що сайт створений зловмисниками [2].

Звичайно, що подібна невтішна статистика ставить перед наукою завдання розвивати нові методи та інструменти для протидії, розслідування шахрайства, скоєного із використанням комп'ютерних технологій, оскільки існують об'єктивні обставини, що ускладнюють проведення досудового розслідування, що полягають у відсутності достатніх знань під час проведення слідчих (розшукових) дій, зокрема пов'язані із оглядом комп'ютерної техніки; недотримання слідчими рекомендацій щодо тактики проведення індивідуальних слідчих (розшукових) дій та призначень експертизи; неналежна взаємодія слідчих з експертними установами. У результаті відсутня науково обгрунтована методологія розслідування шахрайства, вчинене з використанням комп'ютерних технологій, яка негативно позначається на результатах правоохоронної діяльності у цьому напрямі. У зазначеному контексті важливо узагальнити наукові ідеї та підходи до створення якісно нового механізму з метою повного та всебічного розслідування шахрайства з використанням комп'ютерних технологій та попередження нових злочинів.

Стан опрацювання обраної проблематики, аналіз останніх публікацій та досліджень. Беззаперечно, що факт динаміки та розвитку вчинення злочинів у сфері використання інформаційних технологій не залишився поза увагою дослідників, які надали цьому питанню глобалізаційної важливості. Зокрема це такі вчені як: А. І. Анапольська, Р. С. Атаманов, Н. Ю. Кириленко, С. М. Князєв, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, Д.А. Птушкін, В. П. Сабадаш, С.В. Самойлов, М. М. Федотов, К.О. Чередник, С. С. Чернявський, С. В. Шапочка, А. Ю. Юрчук та інші. Навіть при тому, що фішинг вивчався, його складність та багатогранність (наприклад, видами фішингу на сьогодні є: СМС-фішинг, Інтернет-фішинг, вішинг, скімінг, шимінг, онлайн-шахрайство, піратство, мальваре, протиправний контент, рефайлінг та ін.) не дозволяють ефективно протистояти йому без подальших досліджень. Так найбільш «витончені» та інтелектуальні способи вчинення фішингу вимагають

від правоохоронних органів дослідження та розробку нових методів протидії цього злочину.

Мета дослідження полягає у комплексному та ґрунтовному аналізі фішингу як способу вчинення шахрайства у мережі Інтернет із висвітленням головних теоретичних та практичних проблем та пошуку шляхів їх розв'язання.

Виклад основного матеріалу. Фішинг як різновид Інтернет-шахрайства з'явився на початку 1990-х років, що є логічним, оскільки це саме час розвитку інтернет технологій. Концепція була вперше описана в документі 1987 року Джеррі Фелікса і Криса Хаука під назвою «Системна безпека: перспектива хакера». В ньому обговорювався спосіб вчинення злочину «техніка злочинця» та ін. Саме слово переводиться як «риболовля», оскільки воно використовує логіку «приманки», «виманювання даних» [4].

У термінологічному словнику [5, с. 709] під поняттям «фішинг» розуміють вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані – наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [5, с. 709].

Найбільш відома фішинг-атака почалася в мережі America Online (AOL) у 1995 році [4].

Щоб викрасти легітимні облікові дані, зловмисники зв'язувалися з жертвами через AOL Instant Messenger (AIM), видаючи себе за співробітників AOL, які перевіряють паролі користувачів. Термін «фішинг» з'явився в групі новин Usenet, яка зосереджувалася на інструменті AOHell, який автоматизував цей метод, і так ім'я закріпилося. Після того, як AOL в 1997 році ввела контрзаходи, кіберзлочинці зрозуміли, що можуть використовувати таку ж техніку в інших галузях, зокрема й фінансових установах [4].

За цей час кіберзлочинці розробили широкий спектр способів привласнення чужих коштів. Інструментарій шахраїв постійно збільшується, оскільки адекватно реагує на ускладнення телекомунікаційних систем та систем кібер захисту.

За останнє десятиліття кількість користувачів інтернету зросла в рази і продовжує зростати. Одна з причин такого зростання – це смартфони, вони дозволяють легко отримати доступ в інтернет, окрім інших переваг. З іншого боку, фінансові та бізнес-організації, банки, онлайн-магазини використовують інтернет платформи для надання своїх послуг. Проведення фінансових транзакцій через інтернет має ряд переваг, які включають в себе скорочення трафіку, зменшення забруднення повітря, економію часу і грошей і т.д. Однак, не дивлячись на всі переваги використання інтернет ресурсів для фінансових транзакцій і інтернет покупок, на жаль деякі користувачі можуть наражати на небезпеку фінансові операції інших і обманювати їх через фішингові атаки для крадіжки цінної інформації [6].

Фішинг - це комп'ютерна атака, яка передає людям повідомлення соціальної інженерії через електронні канали зв'язку, щоб переконати їх виконати певні дії в інтересах зловмисника [7].

Механізм фішингу полягає в тому, що підроблений сайт, який є майже точною копією справжнього завжди має поле для введення даних. Коли користувач вводить туди свої персональні дані і підтверджує дію, то ці дані відправляються прямо зловмисникові. Далі фішер витягує з них потрібні йому і використовує в своїх цілях. Насамперед атакуючий збирає дані про організацію яку збирається підробляти. Він збирає детальну інформацію на сайті організації і потім використовує її щоб створити підробний сайт [6; 7].

Другий крок атаки - це складання підробного електронного листа. До листа зловмисник прикріплює посилання на фішинговий сайт і розсилає його тисячам користувачів. У тому випадку якщо йде цілеспрямований фішинг, то розсилка іде кільком людям. Поширення шкідливого посилання відбувається не тільки за

допомогою електронної пошти, для цього так само підходять блоги, форуми тощо. Коли користувач відкриває підроблений сайт, він бачить на ньому форму для введення, теж підроблену, найчастіше його просять ввести свої логін і пароль. Він їх вводить, підтверджує і після цього зловмисник отримує доступ до даних жертви. В кінцевому рахунку фішер використовує дані користувача в злочинних цілях, це може бути або крадіжка особистості, або використання кредитної картки для покупок тощо [7].

Так останнім часом спостерігається тенденція до фішинг-атак на банківські та фінансові послуги, електронний банкінг, соціальні мережі, Інтернет-магазини, а також облікові дані електронної пошти, онлайн кабінети користувачів.

Виділяють декілька видів фішингу:

1) Spear phishing (направлений фішинг): цей вид фішингу має конкретного одержувача, групу одержувачів або організацію. Для виконання такої атаки фішер повинен зібрати якомога більше інформації про свої цілі, це може бути заплановане відрядження або замовлення з інтернет-магазину. Цільові атаки мають великий успіх, тому що вони ретельно підготовлені [8].

2) Whaling: атака націлена на керівника підприємства. Інформація від керівника буде завжди більш цінною ніж від звичайного співробітника. В даному випадку підроблений сайт має велику важливість, оскільки представляє певного клієнта організації. Найчастіше фішингових лист складається як суперечність з клієнтом або офіційна проблема, і має виглядати як справжнє бізнес-листування. Атака адаптована для більш обмеженого застосування і найчастіше включає в себе деякі викривлені далекоглядні проблеми [8; 10]. Прикладів використання такого виду є достатньо багато. Так, FACC, австрійський виробник запчастин для літаків, звільнив свого генерального директора через кілька тижнів після звільнення фінансового директора в результаті шахрайства BEC у 2016 році. Компанія втратила близько 55,7 мільйона доларів, коли фішер, який прикидався

генеральним директором, доручив бухгалтерам переказати вказану суму на банківський рахунок для фінансування «проекту придбання» [9].

3) Business email compromise (BEC): атака націлена на співробітників бухгалтерії і відділу фінансів, за допомогою шахрайських дій та з використанням електронної пошти, а також шахрайства з електронною поштою директора. Видаючи себе за значущих людей в компанії, начальника відділу або того ж генерального директора зловмисник провокує співробітників переводити гроші на несанкціоновані рахунки. Як правило, зловмисники компрометують обліковий запис електронної пошти керівника або фінансового директора, використовуючи різні методи. Зловмисник переховується і відстежує дії електронної пошти керівника протягом певного періоду часу, щоб дізнатися про процеси та процедури в компанії. Фактична атака приймає форму помилкового електронного листа, який виглядає так, як ніби воно прийшло з аккаунта керівника(скомпрометованого), відправленого тому, хто є постійним одержувачем. Лист здається важливим і терміновим, і він вимагає, щоб одержувач відправив банківський переказ на зовнішній або незнайомий банківський рахунок. Гроші в кінці-кінців потрапляють на банківський рахунок зловмисника [8; 11 с. 230].

4) Clone phishing(фішинг-клонування): тип атаки при якій фішер клонує вихідне повідомлення, але вкладене в нього посилання замінює на зловмисне. Для цього використовується раніше перехоплене повідомлення і за шаблоном створюється точно таке ж, підробляється відправник. Можливо буде потрібно пояснення чому користувач отримав друге таке саме повідомлення, як правило такою причиною може бути повторна відправка оригіналу або оновлена версія [8].

5) Gaming(ігроманія): ігри стали невід'ємною і поширеною частиною людського взаємодії. У Symatec провели оцінку ігрового простору і виявили, що 13% орієнтовані на застосунки. Ігри в яких відбувається комунікація гравців, як правило вимагають внесення кредитів для просування по рейтингу і

використання деяких функцій. Кредити маються на увазі онлайн внески. Фішингові сайти ловлять клієнтів, пропонуючи неправдиві пропозиції безкоштовних кредитів, орієнтованих на ці ігрові програми [8].

6) Live chat: жертва вводиться в оману запрошенням в живий чат, наприклад на сайтах часто пропонують чат підтримки або питань, чат доданий зловмисником. Цей тип фішингу в основному відбувається на веб-сайті онлайнбанкінгу, де жертва відкриває підроблене вікно чату підтримки в реальному часі на сайті онлайн-банкінгу. Це додає сайту «реальності» і передбачає розкриття конфіденційної інформації жертвою [8].

7) Vishing (телефонний фішинг): має на увазі використання телефону. Як правило, жертва отримує дзвінок з голосовим повідомленням, замаскованим під повідомлення від фінансової установи. Наприклад, повідомлення може попросити одержувача зателефонувати за номером і ввести дані свого облікового запису або PIN-код в цілях безпеки або в інших офіційних цілях. Проте, телефонний номер дзвонить прямо зловмисникові через службу передачі голосу по IP. Останнім часом злочинці стали дзвонити жертвам, прикидаючись технічною підтримкою Apple і надаючи користувачам номер для дзвінка, щоб вирішити «проблему безпеки» [8; 10].

8) Pharming: кібератака, призначена для перенаправлення трафіку сайту на інший, підроблений, сайт. Фармінг може проводитися або шляхом зміни файлу hosts на комп'ютері жертви, або шляхом використання вразливості в програмному забезпеченні DNS-сервера. DNS-сервери – це комп'ютери, що відповідають за перетворення імен Інтернету в їх реальні IP-адреси. Скомпрометовані DNS-сервери іноді називають «отруєними». Фармінг вимагає незахищеного доступу до цільового комп'ютера, наприклад, до зміни домашнього комп'ютера клієнта, а не корпоративного бізнес-сервера.

Крім перерахованих існують й інші види фішингу. За даними компанії PhishMe, 93 % всіх фішингових листів намагались заразити комп'ютер жертви шкідливими програмами криптографічного здирництва - вони шифрують дані на

жорсткому диску та вимагають гроші від жертви за їхнє розшифрування. Також серед стійких тенденцій до підвищення ефективності фішингових атак було назване частіші випадки підлаштування вмісту листів під певну категорію жертв (за їхнім фахом) та із включенням певних елементів особистої інформації (зокрема, звернення до жертви за іменем) [12].

Проаналізувавши судову практику та наукові праці, можна зазначити, що починаючи з 2017 року в України набули широкого прояву шахрайські дій з використанням комп'ютерних технологій, які проявляються у створенні аукціонів, благодійних бірж, продажу неіснуючих товарів на платформах або у соціальних мережах, а також використання фішингових ресурсів, які ззовні схожі на популярні інтернет-магазини, банківські установи або організації.

В Україні фішинг поширений як 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.

Так, у справі № 674/1782/19 Дунаєвським районним судом Хмельницької області встановлено, що з метою власного збагачення, обвинувачений, з власного комп`ютера за допомогою орендованого обладнання хостинг провайдера ТОВ «ТаймВеб» https://timeweb.com створив та розмістив ряд фейкових ресурсів, які імітували можливість перегляду аудіовізуальних творів чи отримання ряду безкоштовних стікерів до соціальних мереж, однак були налаштовані таким чином, що здійснювали викрадення інформації введеної користувачами мережі про власні логіни та паролі доступу до облікових записів. Посилання на фішингові ресурси обвинувачений розповсюджував в соціальній мережі «Вконтакте» https://vk.com, зокрема з облікових записів користувачів аккаунтів здобутих незаконним шляхом [13]. Таким чином злочинець

використовував фішінгові повідомлення з метою привласнення коштів, чим завбав збитків підприємству.

Також відбувається чимало шахрайських дій при 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). Подібну справу розглянула колегія суддів судової палати з розгляду кримінальних справ Апеляційного суду Києва у справі №11-сс796/6258/2017. Організатор злочину купляв на одному з сайтів в Інтернеті ідентифікаційні дані, незаконно зчитані з магнітних стрічок платіжних карток. Цих даних було достатньо для створення дублікатів таких карток та проведення за їх допомогою платежів [14].

Також вироком Стрийського мійськрайонного суду Львівської області по справі № 456/2818/15-к був засуджений громадянин України за ст.190 ч. 3 Кримінального кодексу України, який зареєструвався на сайті aukro.ua, що належить ТзОВ «Аукро 14 Україна» і являє собою електронний аукціон, створив обліковий запис під логіном «ІНФОРМАЦІЯ_2», вказавши при цьому свої власні реєстраційні дані: ім'я користувача потерпілого, з логіном на aukro.ua за адресою місця свого проживання. 24.12.2014 року обвинувачений, маючи умисел на заволодіння чужим майном, будучи учасником електронного аукціону, користуючись логіном «ІНФОРМАЦІЯ_2», під приводом продажу, розмістив оголошення про продаж жіночого взуття «UGGY» за ціною 190 гривень, на інтернет-аукціоні aukro.ua, шляхом обману та зловживання довірою заволодів 24.12.2014 року перерахованими потерпілим грошовими коштами, знявши 190 гривень в банкоматі у м. Стрий, які витратив на власні потреби, а всього завдав потерпілому матеріальної шкоди на суму 190 гривень [15].

Іншим прикладом фішингу «по-українські» є отримання даних про банківську картку та подальше перерахування коштів з банківських карток потерпілого. Для вчинення такого виду шахрайства, через незаконні операції з використанням комп'ютерних технологій, злочинці на сайтах інтернет-торгівлі

підшукують жертв. Так, у справі № 686/26947/19 обвинувачений, скориставшись даними із банківської карти свого знайомого, заволодів коштами на суму 3981 гривню [16].

Актуальним на сьогодні є й 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. Надання послуг через мережу Інтернет останнім часом також набуває популярності й серед громадян. Шахраї на сайтах розміщують інформацію щодо надання послуг з ремонту, купівлі/продажу товару, передачі майна безкоштовно тощо. Після цього, заволодівши грошима чи відповідним майном потерпілих, шахраї не мають наміру їх повертати [17].

Заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину. Наприклад, кримінальне провадження, внесене до ЄРДР за № 12014040000000864. Також, в ухвалі Шевченківського районного суду Чернівців від 29 грудня 2018 року про призначення експертизи згадується викрадення персональних даних користувачів ігрового веб-ресурсу Steam, користувачів соціальної мережі Instagram. Отримання даних акаунтів здійснювалося шляхом брутфорсу (метод хакерської атаки або зламу компютерної системи шляхом перебору всіх можливих комбінацій, які можуть підійти в якості пароля). Також здійснювалося несанкціоноване розповсюдження конфіденційної інформації власників облікових записів поштових сервісів I.UA, Ukr.net, Gmail та інших [18].

З огляду на проведений аналіз судової практики та наукові напрацювання можемо зазначити, що злочиниці, в переважній більшості випадків, зловживаючи довірою, мають на меті заволодінням саме грошовими коштами потерпілих осіб, використовуючи Інтернет-мережу та комп'ютерну техніку.

Важливо, щоб викрадені дані шляхом фішингу використовувалися безпосередньо в ході обману чи зловживання довірою як спосіб заволодіння

грошима. Під час фішингу обман чи зловживання довірою використовується як спосіб доступу до місця зберігання майна, а заволодіння цим майном відбувається в інший спосіб. В абз. 5 п. 17 Постанови зазначається, що за умови, коли обман чи зловживання довірою є лише способами отримання доступу до майна, а саме вилучення майна відбувається таємно або відкрито, то склад шахрайства відсутній [19].

«Слідова картина» є визначальним елементом криміналістичної характеристики таких злочинів, бо її змістом є практичний інструмент як орієнтир при виборі стратегічного напрямку розслідування. Термін «слідова картина» є умовним, оскільки є подібне до поняття «середовище сліду» або «інформаційне середовище». Таким чином, «слідова картина» як елемент криміналістичної характеристики є абстрактною моделлю кримінального злочину, та його слідів, відображених у матеріальному середовищі в результаті його вчинення.

В. Я. Тацій, М. І. Панов, В. Ю. Шепітько, В. О. Коновалова поділяють «слідову картину» більш ширше, як: а) зміни в речовій обстановці; б) сліди-відображення; в) предмети-речові докази; г) ідеальні сліди (сліди пам’яті людини); д) запахові сліди і сліди мікрочастинки [20, с. 194]. В той же час, характерною рисою фішингу як умовного комп'ютерного шахрайства є залишення на місці події слідів іншого типу – віртуальних, що зберігаються у пам'яті електронних носіїв інформації.

Також слід зазначити, що окремими авторами віртуальні сліди визначено як «електронні цифрові сліди», під якими розуміють матеріальні невидимі сліди, які зафіксовані і вивчені за допомогою цифрових електронних пристроїв і мають в собі криміналістично значущу інформацію, що зафіксована в електронній цифровій формі на матеріальних носіях [21]. Такі сліди утворюються після будь-яких дій в інформаційному просторі комп'ютерів їх системах і мережі. Знімки слідів на місці події характеризуються визначеними ознаками, а саме наявністю комп'ютерного обладнання, яке використовувалося потерпілим у

процесі злочинного шахрайства проти нього та містить цифрові сліди, залишені в результаті кримінального злочину.

Стосовно місця події, з якого вчинялося правопорушення з використанням комп'ютерних технологій, то йому характерна наявність наступних предметів, де є сліди правопорушення:

- комп'ютери, їх системні блоки, ноутбуки;

– периферійні пристрої, комунікаційні прилади комп'ютерів і обчислювальних мереж;

– носії інформації;

– засоби зв'язку;

- електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них;
- предмети, отримані після вчинення кримінального правопорушення;
- сліди пальців рук, мікрочастинки або мікрооб'єкти (наприклад, частки волосся), які залишаються на вказаних предметах;
- сліди, що залишаються на «робочому» місці злочинця, (наприклад, які-небудь рукописні записи – списки паролів, коди, чернетки тощо) [21, с. 120].

Проблемі вивчення методів боротьби зі злочинамиу сфері використання цифрових технологій, учені-криміналісти приділяють значну увагу. Дискусії точаться не лише стосовно визначення цифрових слідів кримінальних правопорушень, а й щодо їх найменування [22].

Я. Найдьон у монографії «Поняття та класифікація віртуальних слідів кіберзлочинів» розробив визначення віртуальних або цифрових слідів, яке як ми вважаємоє найбільш влучним. Він вказує, що віртуальні сліди – це електронні сигнали, які залишаються в пам'яті електронних пристроїв, що передаються за допомогою визначеного алгоритму і мають кримінально-релевантне значення [23, с. 305].

Цифровий слід характеризується власними ознаками у вигляді інформаційних елементів, які записані на одному або декількох носіях цифрової інформації. Носії таких слідів підключені до декількох цифрових пристроїв, об’єднаних у телекомунікаційну мережу [24, с. 91].

Втім, найбільш вагома з точки зору отримання неправомірного доступу інформація є саме у доменній адресі (IP-адреси), що дає змогу визначити місцезнаходження точки доступу до комп’ютера, з якого здійснювалося спілкування [24, с. 27].

Переважна більшість шахраїв та їх жертв вибирають електронні платежі через електронні засоби оплати і системи, електронні гаманці та безготівкові платежі. В таких умовах об'єктом відстеження може бути банківська карта, особистий рахунок власника картки.

Особливістю виявлення ідеальних слідів є відсутність безпосереднього контакту між взаємодіючими об’єктами. Оскільки ідеальне відображення здійснюється у формі свідомості, то об’єктом є людина як єдиний носій. У процесі утворення матеріальних слідів об’єктом може також бути людина як тілесна істота [25, с. 7].

Ідеальні сліди скоєння злочину, закріплюються в спеціальних документах, на підставі яких робляться подальші процесуальні дії для ефективного розслідування шахрайства, вчиненого з використанням комп'ютерних технологій.

Таким чином, з огляду на судову практику до слідової картини шахрайства з використанням комп’ютерних технологій слід віднести:

- матеріальні сліди, (80% від досліджених справ) - сліди пальців рук і біологічні сліди, що залишаються комп'ютері та інших засобах, які використовувались під час вчинення шахрайства (на клавіатурі, дисководах, джерелах безперебійного живлення, принтері, робочому місті тощо).
- ідеальні сліди (60 % від досліджених справ). Такі сліди полягають:

– у вигляді певного образу злочинця, який формується у потерпілої особи, оскільки однією із ознак шахрайських дій є саме те, що злочинець намагається увійти у довіру до майбутньої жертви з метою в подальшому привласнити її майно. Для прикладу можемо зазначити справу № 200/12729/18. У данній справі злочинець тривалий час підтримував зв'язок із потерпілою особою та після заволодінням майном ще якийсь час підтримував зв'язок [26];

– у вигляді психологічного ставлення особи злочинця та встановлення його деліктоздатності (в даному випадку виникає необхідність у проведенні судово-психіатричної експертизи) [27].

- цифрові сліди (90 % досліджених справах встановленно наявність цифрових слідів). 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;
- 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.

Для приклада дослідження цифрових слідів можемо зазначити справу №744/1031/18. Зокрема по даній справі проведенно судову комп'ютерно-технічну експертизу, що зумовлено необхідністю підтвердження обставин скоєння злочину з використанням комп'ютерної техніки та для встановлення способу та знаряддя вчиненого шахрайства [28].

Обстановка шахрайств учинених в сфері комп'ютерних технологій відіграє значну роль під час розкриття та розслідування злочину. Під остановкою вчинення зорчину розуміють збіг подій і обставин, за яких вчиняється злочин.

Вона може бути або необхідною ознакою конкретного складу кримінального правопорушення, або обтяжуючою чи кваліфікуючою [29, с. 66].

Інформація отримана із аналізу судової практики вказує на те, що місце проживання злочинця, місце роботи, а також спеціально вибрані місця, злочинець обирає саме ті, 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, можуть вчинятися поза межами нашої держави, а також з тимчасово окупованих територій.

Вироком Кіровського районного суду м. Дніпропетровська від 13.08.2020 по справі 203/1357/19 встановлено, що обвинувачений вдома з метою безкоштовного доступу до мережі Інтернет створив та використав шкідливу комп'ютерну програму, призначену для сканування мережі провайдера й отримання логінів та паролів, для модемного доступу до мережі Інтернет, які містилися на сервері провайдера потерпілого подальшому обвинувачений незаконно використовував логіни та паролі для доступу до мережі Інтернет [30].

Окрім того, з метою приховування IP-адрес злочинці активно використовують спеціальні програми, які не завжди дають змогу правоохоронним органам встановити місце входу в мережу Інтернет [20, с. 269].

Таким чином, місце шахрайства має особливе значення, оскільки є джерелом слідів, що відображають механізм злочину, відносини між злочинцем і жертвою. При цьому, під час розслідування шахрайства місце вчинення кримінального злочину і місце події не завжди є однаковим. Місце вчинення кримінального злочину - одне, а місцем шахрайства виступають кілька пов'язаних місць. Місце вчинення кримінального злочину вибирається з урахуванням можливості здійснення обраного способу вчинення злочину,

предмета посягання, особи потерпілого. Деякі спроби шахрайства можуть мати місце в декількох незв'язаних між собою місцях.

Підводячи підсумки, відзначимо, що місця скоєння шахрайства з використанням комп'ютерних технологій, як правило, являють собою віртуальний простір, відповідно взаємозв'язок між елементами криміналістичної характеристики діяння передбачає, що спосіб шахрайства, його механізм визначаються обстановкою вчинення даного кримінального злочину.

Висновки та пропозиції. До найбільш розповсюджених предметів злочинного посягання слід віднести речі (рухомі й нерухомі) та грошові кошти. Переважна більшість злочинців, які використовували комп’ютерну техніку задля вчинення злочину, мали на меті заволодінням саме грошовими коштами потерпілої особи (80 % від досліджених судових справ).

Визначено найбільш поширені способи фішингу, які умовно можна диференціювати на такі: створення інтернет-аукціонів шляхом надання недостовірних даних та пропозиції продажу неіснуючих товарів; отримання даних про банківську картку та подальше перерахування коштів з банківських карток потерпілого; обманне заволодіння грошовими коштами шляхом створення або використання сайтів благодійних організацій; заволодіння майном шляхом створення і забезпечення діяльності інтернет-магазину.

Зазначено, що залежно від способів учинення шахрайств формуються три групи типових слідів: матеріальні (речові), ідеальні та цифрові. Так, до матеріальних можна віднести сліди пальців рук і біологічні сліди, що залишаються комп'ютері та інших засобах, які використовувались під час вчинення шахрайства (на клавіатурі, дисководах, джерелах безперебійного живлення, принтері, робочому місті тощо).

Цифрові сліди можуть утворюватися: на фізичних носіях комп’ютерної інформації (жорсткі диски, компакт-диски, флешкарти, накопичувачі інформації та ін.); в оперативному запам’ятовуючому пристрої; 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.

Досліджено, що місцем вчинення злочину найчастіше виступає: 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.

Аналізуючи судову практику та накові напрацювання в напрямку злочинів вчинених з використанням комп'ютерних технлогій, можна зазначити, що, здебільшого, для розслідування шахрайства слідчі використовують негласні слідчі (розшукові) дії, найчастіше саме – зняття інформації з технічних каналів зв'язку.

Найбільш розповсюджені слідчі (процесуальні) дії, які проводяться на початковому етапі розслідування шахрайства, вчиненого з використанням комп'ютерних технологій : обшук, огляд предметів вилучених під час проведення обшуку за місцем проживанням підозрюваного, чи іншого помешкання де можуть бути предмети, за допомогою яких здійснювалось досліджене кримінальне правопорушення, допит потерпілого та підозрюваного, призначення судових експертиз.

Визначаючи основні напрями розслідування шахрайств, учинених з використанням комп'ютерних технологій, вказано на необхідність встановлення місця розташування комп'ютерної техніки, з якої здійснювалися дії, пов'язані з незаконним заволодінням чужим майном, з подальшим встановленням осіб, які причетні до такого виду шахрайства.

У процесі розслідування шахрайств, учинених з використанням комп'ютерних технологій, проводяться наступні види експертиз, які найчастіше використовуються згідно проведенного аналізу судових рішень: судова

комп'ютерно-технічна експертиза; судова товарознавча експертиза; економічна експертиза; судово-психіатрична експертиза.

ЛІТЕРАТУРА

1. Сабадаш В.П. Інтернет-шахрайство: реалії сучасності та криміналістичні аспекти протидії. *Ученые записки Таврического национальногоуниверситета им. В. И. Вернадского. Серия : Юридические науки.* 2013. № 1. С. 278-283.

2. Стартував проєкт із протидії кібершахрайству у фінансовому секторі. Офіційне Інтернет-представництво Національного банку України. 2023. URL: https://bank.gov.ua/ua/news/all/startuvav-proyekt-iz-protidiyi-kibershahraystvu-u-finansovomu-sektori. (дата звернення: 15.12.2022).

3. Oreilly L. State of Phishing Report Reveals More Than 255 Million Attacks in 2022. 2022. URL: https://www.slashnext.com/blog/state-of-phishing-report-reveals-more-than-255-million-attacks-in-2022/. (дата звернення: 15.12.2022).

4. What is phishing? ESET. URL:https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/. (дата звернення: 15.12.2022).

5. Чубенко А. Г., Лошицький М. В., Павлов Д. М., Бичкова С. С. та ін. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції. Київ : Ваіте, 2018. 826 с.

6. Phishing Activity Trends Repor. URL: http://docs.apwg.org/reports/apwg_trends_ report_q1_2019.pdf (дата звернення: 15.12.2022).

7. Khonji M. Phishing Detection: A Literature Survey. URL: https://www.researchgate.net/publication/256841808_Phishing_Detection_A_Literature_Survey. (дата звернення: 15.12.2022).

8. Найпопулярніші способи шахрайства в електронній комерції. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-samyepopulyarnye-sposoby-moshennichestva-v-elektronnoj-kommercii. (дата звернення: 15.12.2022).

9. Phishing Spear-Phishing and Whaling – same same but different. Here's how…Computerone. 2018. URL: https://computerone.com.au/phishing-spear-phishing-whaling-whats-difference/.(дата звернення: 15.12.2022).

10. Сабадаш В.П. Фішинг як найбільш розвинений вид шахрайства в інтернеті. Університетські наукові записки. 2006. № 1(17). С. 228-233.

11. Lutkevich B., Casey C., Sharon S. Whaling attack (whaling phishing). TechTarget. URL: https://www.techtarget.com/searchsecurity/definition/ whaling. (дата звернення: 15.12.2022).

12. Korolov M. 93% of phishing emails are now ransomware. 2016. URL: https://web.archive.org/web/20171010005401/https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html. (дата звернення: 15.12.2022).

13. Вирок Дунаєвського районного суду Хмельницької області від 13.12.2019 по справі № 674/1782/19. URL: https://reyestr.court.gov.ua/Review/86357578. (дата звернення: 15.12.2022).

14. Ухвала Апеляційного суду м. Києва від 28.12.2017 по справі № 11-сс/796/6258/2017. URL: https://reyestr.court.gov.ua/Review/72791749. (дата звернення: 15.12.2022).

15. Вирок Охтирського міськрайонного суду Сумської області від 05.03.2021 по справі № 588/1434/17. URL: https://reyestr.court.gov.ua/Review/95355731. (дата звернення: 15.12.2022).

16. Вирок Хмельницького міськрайонного суду Хмельницької області від 29.12.2019 по справі № 686/26947/19. URL: https://reyestr.court.gov.ua/Review/86609811. (дата звернення: 15.12.2022).

17. Вирок Волинського апеляційного суду по справі №166/938/17. URL: https://reyestr.court.gov.ua/Review/72122060. (дата звернення: 15.12.2022).

18. Ухвала Шевченківського районного суду м. Чернівці від 29 грудня 2018 року по справі № 725/3992/14-к. URL: https://reyestr.court.gov.ua/Review/79862106. (дата звернення: 15.12.2022).

19. Про судову практику у справах про злочини проти власності : Постанова Пленуму Верховного Суду України № 10 від 6 листопада 2009 р. URL: https://zakon.rada.gov.ua/laws/show/v0010700-09. (дата звернення: 15.12.2022).

20. Бажанов М. І., Сташис В. В., Тацій В. Я. Кримінальне право України: Особлива частина: підручник. Київ: Юрінком Інтер, 2005. 544 с.

21. Когутич І. І Окремі питання сутності та форм використання спеціальних знань у кримінальному провадженні. *Вісник Академії адвокатури України*. 2015. № 33. С. 112–123.

22. Коментар до ст. 190 Кримінального кодексу України. URL: http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/187.php. (дата звернення: 15.12.2022).

23. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304–307.

24. Коршикова Т. В. Розслідування шахрайства, з використанням електро-обчислювальної техніки. дис. док..філ. 2021. 255 с.

25. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис. … канд. юрид. наук. Харків, 2017. 20 с.

26. Вирок Бабушкінського районного суду м. Дніпропетровська від 20.04.2019 № 200/12729/18. URL: https://reyestr.court.gov.ua/Review/81372099. (дата звернення: 15.12.2022).

27. Вирок Ужгородського міськрайонного суду Закарпатської області від 21.09.2021 по справі № 308/4477/21. URL: https://reyestr.court.gov.ua/Review/99768721. (дата звернення: 15.12.2022).

28. Вирок Менського районного суду Чернігівської області від 01.04.2019 по справі № 744/1031/18. URL: https://reyestr.court.gov.ua/Review/80840782. (дата звернення: 15.12.2022).

29. 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.

30. Вирок Кіровського районного суду м. Дніпропетровська від 13.08.2020 по справі № 203/1357/19. URL: https://reyestr.court.gov.ua/Review/90960245. (дата звернення: 15.12.2022).