УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2024-1/143

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ШАХРАЙСТВ, ВЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

FORENSIC CHARACTERISTICS OF FRAUDS COMMITTED USING INFORMATION COMPUTER TECHNOLOGIES

Ковальський А.В., студент IV курсу
Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка

Стаття присвячена дослідженню окремих аспектів криміналістичної характеристики шахрайств, вчинених із використанням інформаційних комп'ютерних технологій (кібершахрайств).

Визначено, що криміналістична характеристика кібершахрайств – це узагальнена інформаційно-оціночна модель, що включає в себе систематизований опис найбільш типових ознак шахрайств, вчинених із використанням інформаційних комп'ютерних технологій, яка є необхідною для побудови та перевірки слідчих версій і має суттєве значення для виявлення та розслідування даного кримінального правопорушення. Вона включає в себе наступні елементи: спосіб вчинення кримінального правопорушення, відомості про особу злочинця (кібершахрая) та особу потерпілого, а також сліди вчинення. Обґрунтовано, що знання криміналістичної характеристики та її елементів є важливим для досудового розслідування. Зазначені елементи даного кримінального правопорушення можуть перебувати в кореляційному зв'язку. Розкрито значення кожного структурного елементу для криміналістичного документування та досудового розслідування даного кримінального правопорушення.

Досліджено найбільш поширені способи вчинення кібершахрайств. Серед них: фішинг, викрадення та подальше використання персональних даних за допомогою соціальної інженерії та/або програмного забезпечення, використання вразливостей програмного забезпечення потерпілого.

Констатовано, що типовими ознаки особи кібершахрая є: загальні, психологічні, спеціальні. Виокремлено «професійні звички» та «почерк», які допомагають у розслідуванні та ідентифікації злочинця. Запропоновано класифікацію кібершахраїв: особи з різним рівнем навичок у сфері інформаційних комп'ютерних технологій, які раніше не вчиняли кримінальні правопорушення такого виду; особи, які не володіють навичками або мають початковий рівень користування засобами інформаційних комп'ютерних технологій, а також беруть участь у злочинних угрупованнях; особи з високим рівнем навичок у сфері інформаційних комп'ютерних технологій та які систематично вчиняють окреслені кримінальні правопорушення.

Розкрито значення особи потерпілого та його зв'язок із кібершахраєм, а також виокремлено сліди вчинення кібершахрайства та наголошено, що сліди вчинення можуть знаходитися і поза кіберпростором.

Ключові слова: криміналістична характеристика, кібершахрайство, інформаційні комп'ютерні технології, досудове розслідування.

The article is devoted to the study of certain aspects of the forensic characteristics of frauds committed with the use of information computer technologies (cyber frauds).

It was determined that the forensic characteristics of cyber frauds is a generalized information and evaluation model, which includes a systematized description of the most typical signs of frauds committed with the use of information and computer technologies, which is necessary for building a verification of such versions and is of significant importance for detection and investigation this criminal offense. It includes the following elements: the method of committing a criminal offense, information about the identity of the criminal (cyberfraudster) and the identity of the victim, as well as traces of the commission. It is substantiated that knowledge of forensic characteristics and its elements are cases for pre-trial investigation. The specified elements of this criminal offense may be correlated. The meaning of each structural element for criminal legal documentation and pre-trial investigation of this criminal offense is revealed.

The most advanced methods of committing cyber fraud have been studied. Among them: phishing, theft and further use of personal data with the help of social engineering and/or software, use of vulnerabilities in the victim's software.

It was established that the typical characteristics of a cyber fraudster are: general, psychological, and special. «Professional habits» and «handwriting» are singled out, which help in the investigation and identification of the criminal. The classification of cyber fraudsters is proposed: persons with different levels of skills in the field of information and computer technologies who have not previously committed criminal offenses of this type; persons who do not have skills or have an initial level of using information and computer technologies, as well as participate in criminal groups; persons with a high level of skills in the field of information and computer technologies and who systematically commit the outlined criminal offenses.

The significance of the identity of the victim and his connection with the cyber fraudster is revealed, as well as the traces of committing cyber fraud are highlighted and it is emphasized that the traces of the crime can be found outside of cyberspace.

Key words: forensic characteristics, cyber fraud, information computer technologies, pre-trial investigation.

Постановка проблеми. Розвиток інформаційних комп'ютерних технологій спонукає злочинців створювати нові способи вчинення кримінальних правопорушень. В умовах воєнного стану набувають особливої актуальності шахрайства, вчинені із використанням інформаційних комп'ютерних технологій (кібершахрайства). Дані протиправні діяння не тільки завдають матеріальної шкоди громадянам, а й наносять репутаційних втрат нашій державі.

Так, використовуючи засоби інформаційно-комп'ютерних технологій та створені фейкові акаунти у соціальній мережі Facebook, особа розміщував неправдиві повідомлення про збір коштів на лікування хворих дітей та поранених військовослужбовців [1].

В іншому випадку особи створили міжнародний псевдоінвестиційний фонд «S-Group». Вони пропонували потерпілим пасивний дохід шляхом інвестицій в криптовалюту. Для користування своїми послугами створили власний фінансовий криптогаманець, на який потерпілі переказували кошти, купуючи їх фіктивні віртуальні активи (криптовалюту). У подальшому шахраї переводили отримані кошти на власні рахунки, а згодом зникли. Даними протиправними діями вони завдали великих матеріальних збитків громадянам різних країн [2].

Зважаючи на це, важливим є розробка сучасних методик розслідування шахрайств, вчинених з використанням інформаційних комп'ютерних технологій (кібершахрайств).

Аналіз останніх досліджень. Проблемні питання розслідування кібершахрайств досліджувалися в працях наступних вчених: А. І. Анапольської, О. В. Бишевець, Л. В. Годнюк, С. О. Єгорова, Я. В. Неділька, Н. В. Павлової, Т. В. Романенко, С. В. Чучко, О. О. Юхно та інших. Окремо варто зазначити роботу С. В. Самойлова, який

виокремив класифікацію шахрайств, вчинених із використанням мережі Інтернет за способом, а також розглянув процес слідоутворення у даних кримінальних правопорушеннях [3]. Не можна оминути роботу Н. В. Сметаніної, Д. О. Пісенка та Т. А. Дібрової де були проаналізовані основні тенденції вчинення кібершахрайств в умовах воєнного стану [4]. Серед зарубіжних науковців варто виділити роботу E. Btoush, R. Genrich та P. Sankarah, які дослідили особливості вчинення кібершахрайств, пов'язаних із використанням банківських карток [5].

Метою статті є дослідження криміналістичної характеристики шахрайств, вчинених із використанням інформаційних комп'ютерних технологій (кібершахрайств).

Виклад основного матеріалу. Відповідно до статистики Офісу Генерального прокурора, протягом 2021 року було обліковано 14760 кримінальних правопорушень, передбачених ч. ч. 2–4 ст. 190 КК України, у 2022 році – 19430, у 2023 – 53547. Наведена статистика підтверджує той факт, що вчинення шахрайств, у тому числі з використанням інформаційних комп'ютерних технологій, стрімко збільшується [6]. Саме тому існує необхідність у дослідженні криміналістичної характеристики даних протиправних діянь, що буде сприяти їх ефективному розслідуванню, встановленню винних осіб та притягненню їх до кримінальної відповідальності.

У теорії криміналістики існує велика кількість підходів щодо визначення поняття «криміналістична характеристика кримінального правопорушення». Зокрема, В. П. Берназ зазначив, що вперше у 1967 році термін «криміналістична характеристика злочину» був застосований О. Н. Колесніченком в докторській дисертації «Наукові та правові основи розслідування окремих видів злочинів» (Харків). Автор до найбільш важливих положень методики розслідування відносить «криміналістичну характеристику злочину». Однак, не розкриває змісту даного поняття [7, с. 31]. Дотепер серед вчених-криміналістів не існує єдності стосовно тлумачення поняття криміналістичної характеристики.

Погоджуємося із визначення запропонованим М. А. Погорецьким та Д. Б. Сергєєвою, які криміналістичну характеристику кримінальних правопорушень розглядають як «інформаційну модель типових ознак певного виду (групи) кримінальних правопорушень, яка відображає закономірні зв'язки між цими ознаками та дозволяє обрати необхідну методику та засоби розслідування» [8, с. 25].

Досліджуючи елементний склад криміналістичної характеристики кібершахрайств, вважаємо, що до нього необхідно відносини: 1) спосіб вчинення; 2) відомості про особу потерпілого та особу злочинця; 3) сліди вчинення.

Зазначимо, що спосіб вчинення кібершахрайства залежить від багатьох факторів: масштабу злочинного діяння, наявністю у особи злочинця відповідних (спеціальних) знань та самої особи потерпілого. Наприклад, найбільший успіх злочинці отримали під час вчинення шахрайств з використанням інформаційних комп'ютерних технологій, направлених на осіб у віці від 18–40 років, які працюють у сфері фінансів або IT [9; 10].

Оскільки спосіб вчинення даного кримінального правопорушення може змінюватися з часом та розвитком інформаційних комп'ютерних технологій, зауважимо про найбільш поширені з них:

1) *фішингові атаки* – надсилання електронних повідомлень, які містять посилання на фейкові веб-сайти. Метою є змусити особу надати свою конфіденційну інформацію (паролі, номера кредитних карто тощо). Злочинці створюють веб-сайти, які точно імітують зовнішній вигляд законних веб-ресурсів. Наприклад, організована група з Харкова, використовувала рекламні засоби в соцмережах для привертання уваги осіб, зацікавлених у грошовій допомозі від держави чи благодійних фондів. Дана реклама включала посилання на офіційний державний портал для отримання допомоги. Перейшовши за даним посиланням, потерпілі потрапляли на шахрайський сайт, що імітував офіційний онлайн-банкінг. Громадяни вводили реквізити своєї банківської картки, які потім ставали доступними шахраям [11].

Також, поширеними є випадки створення коллцентрів. Зловмисники у Львівській, Одеській, Дніпропетровській та інших областях використовували фішинг для отримання конфіденційної інформації про потерпілих, а потім шляхом обману змушували осіб здійснювати перекази на банківські рахунки злочинців [12];

2) *викрадення та подальше використання особистих даних за допомогою соціальної інженерії та/або програмного забезпечення*. Одним із варіантів отримання особистих даних за допомогою програмного забезпечення є використання брутфорс (автоматизоване програмне забезпечення для підбору паролей), якщо зловмиснику відомі початкові дані потерпілої особи.

Нерідко, злочинці використовують методи соціальної інженерії. Вироком Івано-Франківського міського суду від 28.03.2019 року № 344/17229/17 було встановлено, що фахівець банку здобула конфіденційну інформацію про персональні дані власника банківської платіжної картки, зокрема фінансовий номер телефону клієнта банку, а також логін і пароль доступу до розрахункового рахунку. Під час телефонної розмови, видаючи себе за клієнта банку отримала незаконний доступ до банківських коштів потерпілого та здійснила декілька переказів його коштів на свої рахунки [13];

3) *використання вразливостей програмного забезпечення потерпілого.* Кібершахраї можуть використовувати відомі вразливості системи безпеки програмного забезпечення або операційних систем, щоб отримати несанкціонований доступ до засобів інформаційних комп'ютерних технологій. Даний спосіб використовується для викрадення конфіденційних даних, встановлення або створення бекдору, яке дозволяє зловмиснику в будь-який час отримувати доступ до операційної системи. Прикладом може слугувати так звана «атака Сибіли», яка є загрозою безпеці онлайн-системи, де відбувається захоплення мережі, за допомогою облікових записів, вузлів або комп'ютерів [14].

Варто згадати нещодавню хакерську атаку на мережу «Київстар», яка була здійснена за схожим принципом [15].

Як наслідок, після таких атак, злочинці отримують базу даних клієнтів та їх персональні дані, що можуть у подальшому використовуватися у протиправних цілях як знаряддя або джерело для вчинення шахрайських дій.

Що стосується приховування кібершахрайств, то в переважній більшості злочинці використовують анонімайзери – це спеціальні програми, які дозволяють замаскувати місцезнаходження під час протиправних дій. До прикладу, Tor або DarkWallet. Останній найчастіше застосовується у сфері віртуальних активів.

Наступним елементом криміналістичної характеристики шахрайств, вчинених із використанням інформаційних комп'ютерних технологій, є характеристика особи злочинця (кібершахрая).

Зауважимо, що криміналістична інформація стосовно кібершахрая дає змогу органам досудового розслідування з'ясувати його характерні ознаки, можливі мотиви та сліди вчинення кримінального правопорушення, а також обрати відповідну тактику проведення окремих слідчих (розшукових) дій.

Загалом, аналіз різних криміналістичних точок зору дає змогу виокремити ознаки, які характерні для особи кібершахрая. До таких ознак доцільно відносити:

1) загальні (етнічне походження, вік, освіта, професія);

2) психологічні (темперамент, характер, інтереси та схильності, мотиви та стиль поведінки, певні психічні відхилення);

3) спеціальні («професійні звички» та «почерк» кібершахрая) [16, с. 207].

Прикладом професійної звички кібершахрая може бути: 1) використання конкретного програмного забезпечення для анонімності (VPN, проксі-сервера); 2) певний спосіб вчинення кримінального правопорушення (фішинг, брутфорс); 3) спосіб отримання конфіденційних даних про особу потерпілого (самостійний, купівля відповідних баз даних в мережі Інтернет); 4) використання операційної системи, певної марки техніки, програмної мови.

На відміну від «професійної звички», «почерк» кібершахрая – це характерна дія, яку особа свідомо вчиняє, розуміючи, що цим вона виокремлює себе серед інших [17, с. 103]. Це може бути як спосіб написання повідомлень, так і аватарка на відповідних форумах.

Кібершахраїв можна умовно поділити на три групи:

– особи з різним рівнем навичок у сфері інформаційних комп'ютерних технологій, які раніше не вчиняли кримінальні правопорушення такого виду;

– особи, які не володіють навичками або мають початковий рівень користування засобами інформаційних комп'ютерних технологій, а також беруть участь у злочинних угрупованнях;

– особи з високим рівнем навичок у сфері інформаційних комп'ютерних технологій та які систематично вчиняють окреслені кримінальні правопорушення.

Знання рівня підготовки або почерку злочинця може надати інформацію слідчому про місце знаходження слідів вчинення кримінального правопорушення. Наприклад, якщо є відомості про те, що особа використовує незахищену IP-телефонію (наприклад Zoiper), можна зробити висновок, що вона не володіє високим рівнем навичок у сфері інформаційних комп'ютерних технологій та може знаходитися у складі організованої злочинної групи (так званих шахрайських колл-центрів).

Досліджуючи вітчизняну криміналістичну літературу [1; 18; 19], можна виокремити специфічні ознаки, які характерні для особи потерпілого.

Зокрема, важливою ознакою є вік потерпілої особи, оскільки фішинг, як спосіб вчинення кібершахрайства, найчастіше може бути застосований саме до літніх людей.

Наступною ознакою можна вважати місцезнаходження потерпілої особи. До прикладу, зателефонувавши потерпілому в нічний час доби, можна його дезорієнтувати та виманити конфіденційні дані банківських карток.

Варто зауважити й про кібершахрайство щодо юридичних осіб (як правило це банківські установи, криптовалютні біржі або державні установи). Так, хакер Гонзалес із США отримав конфіденційну інформацію щодо заходів безпеки від десятків мільйонів кредитних карток із різних фінансових установ. Після чого, він зламав мережу банків та використовуючи раніше отримані дані, представлявся потерпілим та здійснював перекази на свої власні рахунки [20].

Не менш важливим елементом криміналістичної характеристики кібершахрайства є сліди їх вчинення. У теорії криміналістики традиційно виділяють два види слідів: матеріальні та ідеальні. Матеріальні сліди – зміни в елементах речової обстановки, що виникають як результат механічного, хімічного, біологічного, термічного та іншого впливу. Ідеальні сліди – відображення криміналістично значущої інформації у свідомості людей, що зберігається в пам'яті людини [21, с. 220]. Матеріальними слідами даного кримінального правопорушення можуть бути: сліди-відображення зовнішнього фізичного впливу на інформаційні комп'ютерні технології (сліди рук, ніг, знарядь злому тощо); сліди-речовини у вигляді витратних матеріалів (тонерів, фарб, різних мастил, що використовують у комп'ютерних системах, їх мережах і периферичних пристроях); сліди-предмети – змінні диски та стрічки, пристрої дистанційного зняття інформації, роздруківки на паперових носіях і документи на електронних носіях, кабелі та роз'єми, пристрої фізичного знищення комп'ютерів, їх мереж [22]. Ідеальні сліди можуть залишатися в пам'яті людини та становити інформацію про наслідки вчинення кібершахрайства, його спосіб, дані про особу злочинця.

У науковій літературі тривають дискусії з приводу виокремлення третього виду слідів – електронних, при цьому пропонуються різні їх визначення. Підтримуємо позицію Н.М. Ахтирської, що електронна інформація не належить у чистому вигляді ні до матеріальних слідів, ні до ідеальних, але при цьому має деякі схожі з ними ознаки [23, с. 136–137].

Електронні сліди вчинення кібершахрайства можуть залишатися у комп'ютері, пристроях зберігання даних та безпосередньо у комп'ютерній мережі. Важливе значення для розслідування даного кримінального правопорушення становлять відомості від інтернет-провайдера, а саме інформація про події, які відбувалися в мережі Інтернет. Якщо кібершахрай використовував шкідливе програмне забезпечення, то потрібно досліджувати тимчасові файли, які були залишені на засобі інформаційно-комп'ютерної технології потерпілого. Сліди вчинення кібершахрайства можуть знаходитися і поза кіберпростором. Зокрема, матеріальні сліди знищення пристроїв або ж серверів.

Висновки. Криміналістична характеристика кібершахрайств має важливе практичне значення для органів досудового розслідування, оскільки слугує підґрунтям висунення версій та дозволяє обрати відповідну тактику проведення окремих слідчих (розшукових) дій під час розслідування зазначених кримінальних правопорушень.

У зв'язку із збільшенням кількості вчинення окреслених протиправних діянь, необхідно розробляти нові рекомендації, засоби і методи їх розслідування.

ЛІТЕРАТУРА

1. Підозрюваного у шахрайстві волинянина, який виманив понад чверть мільйона гривень на лікування неіснуючих військових, взяли під варту. *Волинська обласна прокуратура*. URL: https://vol.gp.gov.ua/ua/news.html?_m=publications&_c=view&_t=rec&id=337170(дата звернення: 18.01.2024).

2. Омельченко В. Фінансова "піраміда": Нацполіція шукає потерпілих від шахрайського проєкту "S-Group" | УНН. *Оперативні новини України та Світу | Українські Національні Новини УНН*. URL: https://unn.ua/news/finansova-piramida-natspolitsiia-shukaie-poterpilykh-vid-shakhraiskoho-proiektu-s-group(дата звернення: 20.01.2024).

3. Самойлов С. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 081. Донецьк, 2014. 18 с. URL: https://dspace.nlu.edu.ua/handle/123456789/14174(дата звернення: 18.01.2024).

4. Dibrova T. A., Pisenko D. O., Smetanina N. V. Cybercrime and cyberfraud under martial law. *Juridical scientific and electronic journal*. 2022. No. 11. P. 546–549. URL: https://doi.org/10.32782/2524-0374/2022-11/132(дата звернення: 18.01.2024).

5. A systematic review of literature on credit card cyber fraud detection using machine and deep learning / E. A. L. Marazqah Btoush et al. *PeerJ computer science*. 2023. Vol. 9. P. e1278. URL: https://doi.org/10.7717/peerj-cs.1278(дата звернення: 18.01.2024).

6. Карчевський М. Протидія злочинності в Україні : інфографіка : інтерактивний довідник. Версія 3.0. URL : https://karchevskiy.com/i-dovidnyk/(дата звернення: 18.01.2024).

7. Берназ П. Поняття «Криміналістична характеристика злочину». *Південноукраїнський правничий часопис*. 2017. С. 30–34. URL: http://www.sulj.oduvs.od.ua/archive/2017/2/11.pdf(дата звернення: 18.01.2024).

8. Погорецький М., Сергєєва Д. Розслідування окремих видів злочинів : навч. посіб. Київ : Алерта, 2015. 536 с.

9. The latest phishing statistics (updated january 2024) | AAG IT support. *AAG IT Services*. URL: https://aag-it.com/the-latest-phishing-statistics/(дата звернення: 18.01.2024).

10. Top phishing statistics for 2024: latest figures and trends. *StationX*. URL: https://www.stationx.net/phishing-statistics/#:~:text=An%20estimated%203.4%20billion%20emails,of%20all%20email%20traffic%20globally(дата звернення: 18.01.2024).

11. На Харківщині судитимуть шахраїв, які заробляли на фішингу. *"Інфосімі" – інформаційно-аналітичний портал*. URL: https://izvestia.kharkov.ua/proisshestvija/na-kharkivshchyni-sudytymut-shakhraiv-iaki-zaroblialy-na-fishynhu/(дата звернення: 18.01.2024).

12. Interfax-Ukraine. Кіберполіцейські припинили діяльність шахрайських call-центрів у трьох областях України. *Інтерфакс-Україна*. URL: https://interfax.com.ua/news/telecom/932427.html(дата звернення: 18.01.2024).

13. Вирок Івано-Франківського міського суду від 28.03.2019 р. у справі № 344/17229/17. URL: https://verdictum.ligazakon.net/document/80766905?q="з%20використанням%20електронно-обчислювальною%20техніки"(дата звернення: 18.01.2024).

14. Academy B. Sybil attacks explained | binance academy. *Binance Academy*. URL: https://academy.binance.com/en/articles/sybil-attacks-explained(дата звернення: 18.01.2024).

15. Ukrinform. Збій у роботі «Київстару» стався через потужну хакерську атаку. *Укрінформ – актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-technology/3799022-zbij-u-roboti-kiivstaru-stavsa-cerez-potuznu-hakersku-ataku.html(дата звернення: 18.01.2024).

16. Неділько Я. Типові ознаки кіберзлочинця (криміналістичний аспект). *Держава і право*. 2020. № 88. С. 202–211. URL: https://derzhava-i-pravo.com.ua/files/issues/State%20and%20Law.%20Issue%2088.pdf#page=202(дата звернення: 18.01.2024).

17. Неділько Я. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій : дис. … д-ра філософії в галузі права : 12.00.09. Київ, 2023. 257 с. URL: https://scc.knu.ua/zdobuvach-phd?id=335895(дата звернення: 18.01.2024).

18. Kuchynska O. The person of the victim as an element of the criminal characteristics of criminal offenses committed with the use of information technologies. *Uzhhorod national university herald. series: law*. 2023. Vol. 2, no. 77. P. 240–244. URL: https://doi.org/10.24144/2307-3322.2023.77.2.41(дата звернення: 18.01.2024).

19. Kuzmenko O. V. Features of criminalistic characteristics of cyber crimes. *Actual problems of native jurisprudence*. 2022. No. 4. P. 162–166. URL: https://doi.org/10.32782/39221335(дата звернення: 18.01.2024).

20. IT leadership – ARN. *ARN*. URL: https://www.arnnet.com.au/it-leadership/(дата звернення: 18.01.2024).

21. Благута Р., Гарасимів О., Дуфенюк О. Криміналістика : підручник / Заг. ред. Є. Пряхін. 3-тє вид. Львів : ЛьвДУВС, 2016. 948 с.

22. Паламарчук Л. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. … канд. юрид. наук : 12.00.09. Київ, 2004. 215 с.

23. Ахтирська Н. Актуальні питання розслідування кіберзлочинів : навч. посіб. Київ : Київ. ун-т, 2018. 229 с.