УДК 34

Виды следов, способствующих установлению лица, совершившего дистанционное мошенничество

Кулаевский Андрей Витальевич

Аспирант кафедры уголовного процесса и криминалистики,
Юридический институт Алтайского государственного университета,
656049, Российская Федерация, Барнаул, просп. Социалистический, 68;
e-mail: andrei8888.98@mail.ru

Аннотация

В статье исследуются следы, оставляемые преступником при совершении дистанционного мошенничества. Автором приводятся различные классификации следов преступления, образующихся в информационной среде. Указываются основные цифровые следы, оставляемые преступником в момент совершения преступления. Особое внимание уделяется следам, позволяющим установить лицо, совершившее дистанционное мошенничество. Выводы подтверждаются примерами из судебно-следственной практики. В дополнении к имеющемся в науке цифровым следам автором выделяются следы в виде информации о входящем и исходящем трафике конкретного IP-адреса, хранящейся у интернет-провайдера или системного администратора, а также протоколы работы пользователей в сети Интернет с указанием подключений. Выделяются три группы следов дистанционного мошенничества, содержащих информацию о лице, его совершившем.

Для цитирования в научных исследованиях

Кулаевский А.В. Нормативно-правовые основания развития программы материнского (семейного) капитала // Вопросы российского и международного права. 2024. Том 14. № 7А. С. 449-456.

Ключевые слова

Следы преступления, классификации следов, установление лица, совершившего преступление, дистанционное мошенничество, информационная среда.

Введение

Хищения, совершенные с использованием информационного-телекоммуникационных технологий, занимают значительное место в ежегодной статистке зарегистрированных преступлений. В соответствии с данными МВД о состоянии преступности в России, в 2023 году их зарегистрировано 677 тыс., что на 29,7% больше, чем в 2022 году. Возрос их удельный вес в структуре преступности: с 26,5% в 2022 г. до 34,8% в 2023 г. Более чем три четверти таких преступлений (77,8%) совершается с использованием сети Интернет, почти 44,7% – средств мобильной связи. В числе указанных высокотехнологичных преступлений 356 тыс. (52,6%) составляют мошенничества (прирост в 2023 г. – 38,2%), а раскрываемость их составляет всего 24,5% при общей раскрываемости преступлений 52,3% [Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года, www].

Ежегодное увеличение количества совершаемых преступлений и их низкая раскрываемость, на наш взгляд, обусловлены несколькими причинами:

1. Широким распространением механизмов дистанционного банковского обслуживания. Преступники используют уязвимые звенья механизмов для своих противоправных целей.

2. Появлением технологий, позволяющих осуществлять преступную деятельность анонимно, подменяя имя, IP-адреса, номера мобильных телефонов.

3. Взаимодействие потерпевшего с мошенником осуществляется дистанционно, посредством телефонной связи, обмена сообщениями в социальных сетях, мессенджерах.

4. Предмет преступления – безналичные денежные средства, являющиеся для преступника удобным предметом хищения, легко скрываются, так как в дальнейшем перемещются на различные электронные кошельки.

Несмотря на то, что правоохранительные органы фиксируют указанные преступления и, как следствие, возбуждают большое количество уголовных дел, качество предварительного расследования нельзя оценить положительно, особенно в части установления лица, совершившего дистанционное мошенничество. Свидетельство этому – приведенные выше статистические данные. Одновременно с возросшим количеством совершенных преступлений растет число уголовных дел, производство по которым приостановлено в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

В связи с этим научный интерес и практическую значимость представляет изучение следов, оставленных преступником при совершении дистанционного мошенничества, так как именно они являются основными источниками информации, способствующими его установлению.

Основное содержание

В науке неоднократно предпринимались попытки определить и классифицировать различные следы преступления, оставленные в информационной среде.

В.А. Мещеряковым было предложено ввести понятие «виртуальный след», Л.Б. Краснова определяет понятие «электронно-цифровой объект», Г.М. Шаповалова, В.В. Борисов, Ю.В. Гаврилина определяют понятие «информационного следа», Н.Н. Лыткин рассматривает понятие «компьютерно-технические следы», В.А. Милашев определяет понятие «бинарные следы», В.Б. Вехов – «электронно-цифровой след», Е.Р. Россинская определяет понятие «цифровой след».

При наименовании следов, оставляемых в информационном пространстве, нам близка

позиция Е.Р. Россинской и И.А. Рядовского, выделяющих понятие «цифровой след» и представляющих его как «...криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [Россинская, Рядовский, 2019].

Всё же в рамках настоящего исследования важной особенностью для определения понятия и выделения классификаций следов является направленность на получение информации о преступнике исключительно в целях установления его личности.

Вполне обоснована позиция И.Ф. Крылова, указывающего, что классификация следов призвана служить практическим целям, поэтому должна быть научной и достаточно простой [Крылов, 1976, 32].

Необходимо отметить, что в криминалистической науке приведен обширный перечень классификаций следов, но, к сожалению, не все из них позволяют выделить следы, указывающие на лицо, совершившее преступление.

Для того чтобы подтвердить значимость высказанной И.Ф. Крыловым позиции, приведем классификации с выделением цифровых следов, непосредственно отвечающих практическим задачам деятельности следователя по установлению лица, совершившего дистанционное мошенничество.

При установлении преступника для следователя важны только те следы, которые могут содержать информацию, позволяющую собрать достоверные сведения о личности преступника.

В настоящее время в науке представлены различные классификации, имеющие разное содержание, не всегда указывающее на пользователя как на следоотображающий и следовоспринимающий объект.

А.Л. Осипенко предлагает использовать классификацию по способу создания цифровых данных в виде файлов: 1. Файлы, созданные пользователем и сохраненные на материальном носителе устройства. 2. Файлы, созданные в автоматическом режиме без участия пользователя. 3. Файлы, в которых записи могут быть сгенерированы устройством с учетом управляющих последовательностей, определенных пользователем [Колычева, 2018].

Прикладное значение указанной классификации заключается в изучении цифрового следа, оставленного пользователем, а значит непосредственно указывающего на него.

А.А. Жижилева дифференцирует виртуальные следы на два основных вида: активные – сознательная деятельность субъекта в информационно-телекоммуникационном пространстве (переписка, ведение блогов, комментарии) и пассивный виртуальный след – совокупность данных, оставленных пользователем непреднамеренно (история посещения сайтов, IP-адрес и т.д.) [Жижилева, 2019].

Представленная классификация интересна тем, что позволяет обратить внимание на следы, оставленные преступником непроизвольно, что позволит собрать дополнительную информацию о личности преступника.

Схожая классификация представлена в работе А.Г. Себякина. Предлагается классификация цифровых следов по степени воздействия пользователя на компьютерную систему [Себякин, 2021]. По мнению автора классификации, такие следы делятся на непосредственные и опосредованные. Под непосредственными следами в указанном случае следует понимать электронно-цифровые следы, возникающие в результате непосредственного воздействия пользователя на компьютерную систему. Указанные следы могут находиться как непосредственно на материальном носителе электронного устройства, так и вне его (доступ к которым обеспечивается с применением средств телекоммуникации, т.е. канала связи).

Под опосредованными следами автор понимает цифровые следы, образованные в результате функционирования системного программного обеспечения, стандартами форматов файлов и протоколов передачи данных вне зависимости от воли пользователя [Старостенко, 2023].

Изучение таких классификаций позволяет обозначить блоки информации, собираемые информационной средой принудительно, в виде метаданных. К примеру, история посещений веб-сайтов, время использования сети Интернет, информация о собранных Cookies-файлах.

Интерес вызывает классификация, приведенная Н.И. Старостенко в своем диссертационном исследовании. Автор разделяет электронно-цифровые следы в зависимости от источника извлечения информации – электронное устройства потерпевшего и преступника [Старостенко, 2023, 104.].

Важными являются и классификации, указывающие на место нахождения цифрового следа. В.В. Вехов указывает, что электронно-цифровые следы могут быть подразделены на следующие виды: 1) следы-отображения: электромагнитные сигналы, файлы, компьютерные программы, базы данных, электронные сообщения, электронные документы, электронные страницы в сети ЭВМ (компьютерной сети), сайты в сети Интернет; 2) следы-предметы: машинные носители информации, интегральные микросхемы и микроконтроллеры, ЭВМ (компьютеры), системы ЭВМ (компьютерные системы), сети ЭВМ (компьютерные сети) [Вехов, 2008, 81].

Интересна классификация цифровых следов по источнику их хранения, представленная А.Н. Колычевой [Колычева, 2018]: Автор разделяет 1. Следы на жестких дисках (HDD, SDD), flash-накопителях (SD, MMC и прочих), USB-накопителях, оптических носителях (CD, DVD, BD), магнитных носителях (Floppy, Zip, магнитных лентах); 2. Следы, находящиеся в оперативной памяти ЭВМ, периферийных устройств и средств связи. 3. Следы в проводных, радио, оптоволоконных и иных электромагнитных системах связи.

Представленные классификации также имеют прикладное практическое значение, так как непосредственно указывают на место нахождения цифровых следов и источник их хранения, что позволяет следователю охватить большее количество следовоспринимающих и следоотображающих объектов при сборе информации, пригодной для установления лица, совершившего преступление.

Кроме классификаций в науке, представлены разнообразные виды следов, оставляемых преступником, выделение которых также зависит от способа совершения преступления.

Ввиду большого количества способов совершения дистанционного мошенничества мы согласны с классификацией способов хищений, совершенных с использованием интернет-технологий, приведенных И.Е. Мазуровым, выделившим группу способов «дистанционный доступ к машинным носителям и информации» [Мазуров, 2017].

Ввиду того, что дистанционный способ совершения мошенничеств возможен только с использованием технических средств, имеющих доступ в Интернет, следы преступления формируются и остаются на таком техническом устройстве и в информационной среде.

Дистанционная группа способов совершения мошенничеств имеет схожие цифровые следы. О.С. Буденко [Буденко, 2016] и А.В. Шебалин [Шебалин, 2010, 153] выделяют следующие следы, оставленные при использовании сотового телефона: следы, отображающиеся в электронной памяти сотового телефона и в информационной системе оператора сотовой связи. Такими следами, по мнению автора, могут быть: 1) следы телефонных переговоров; 2) следы передачи и приема сообщений; 3) следы доступа в сеть Интернет и использования предоставленных там услуг; 4) следы, образуемые в результате внесения записей об абонентах в записную книгу; 5) следы, содержащиеся в аудио, фото и видеозаписи; 6) следы в финансовых

операциях; 7) следы в специальных программных средствах для прошивки мобильных телефонов и SIM-карт; 8) следы в приложениях Viber, Skype, WhatsApp, Facebook, Vkontakte и др., в которых могут содержаться данные пользователей мобильных телефонов, IMEI-код, фотографии и видеозаписи.

В дополнении могут быть добавлены следующие следы: информация о входящем и исходящем трафике конкретного IP-адреса, хранящаяся у интернет-провайдера или системного администратора, а также протоколы работы пользователей в сети Интернет с указанием подключений.

Проанализировав вышеприведенные классификации и виды следов, представим собственную классификацию цифровых следов.

В целях установления лица, совершившего преступление, нами предлагается разделить цифровые следы на следующие группы: следы, способствующие установлению личности преступника; следы, способствующие установлению места нахождения преступника; следы, способствующие получению диагностической информации о признаках и свойствах личности преступника.

К первой группе относятся следы, имеющие или позволяющие получить информацию о лице, совершившем преступление, в том числе следы, указывающие на анкетные персональные данные пользователя, а также активность посещения сайтов пользователя (файлы с персональными данными и файлами cookies); цифровые идентификаторы оконечного оборудования, информационных систем и компьютерных сетей (IP-адрес, доменное имя сайта).

К примеру, приговором Ленинского районного суда г. Иваново Ивановской области в качестве доказательств, подтверждающих вину подсудимого, исследован ответ на запрос в АО «Киви Банк». К ответу на запрос приложены цифровые следы, имеющие информацию о преступнике CD – диск с файлом «.xls», в котором имеется таблица с информацией об аккаунте, в которой указаны:дата создания кошелька; дата последнего входа; IP последнего входа, имя владельца электронного кошелька (от 04 августа 2023 г. № 1-182/2023 по делу 1-182/2023, использованы данные интернет-ресурса sudact.ru).

Ко второй группе относятся следы, указывающие на местонахождение компьютерного устройства в случае неиспользования им серверов удаленного доступа (VPN). Такие следы содержатся в базовых станциях оператора мобильной связи, а также в сервере провайдеров, обеспечивающих преступника доступом к интернету.

Приведем пример. Приговором Ленинского районного суда г. Красноярска Красноярского края от 27 февраля 2023 г. в качестве доказательства, подтверждающего вину подсудимого, представлен протокол осмотра документов, согласно которому осмотрен документ, предоставленный ПАО «ВымпелКом» с информацией о наличии соединения между абонентскими номерами мошенника и преступника, с указанием местоположения таких устройств (приговор от 27 февраля 2023 г. № 1-16/2023 по делу № 1-16/2023, использованы данные интернет-ресурса sudact.ru).

В третью группу включаются следы, имеющие биологические, социальные и психологические свойства и позволяющие в ходе исследования получать диагностическую информацию о лице, совершившем преступление.

К таким следам относятся следы пальцев рук на слипах, чеках, SIM-карте, мобильном телефоне (дактилоскопическая экспертиза); запись голоса мошенника, хранящаяся у оператора сотовой связи (фоноскопическая экспертиза), файлы с речевыми следами (лингвистическая экспертиза).

Так, приговором Свердловского районного суда г. Белгорода Белгородской области доказательствами, подтверждающими вину подсудимого, признаны результаты проведенных оперативно-розыскных мероприятий. В ходе осмотра и прослушивания фонограммы телефонных переговоров установлено содержание разговоров между мошенниками. В материалах уголовного дела содержится оптический диск с результатами ОРД – «прослушивание телефонных переговоров», который признан вещественным доказательством и приобщен к уголовному делу. Принадлежность голоса подсудимого подтверждена заключением фоноскопической экспертизы (приговор от 04 августа 2023 г. № 1-110/2023 по делу № 1-110/2023, использованы данные интернет-ресурса sudact.ru).

Заключение

Таким образом, в зависимости от поискового потенциала целесообразно выделять три группы следов дистанционного мошенничества, содержащих информацию о лице, его совершившем. Поиск представленных следов составляет значительную часть деятельности следователя по установлению преступника. Выполняя свою деятельность, следователь выявляет и изучает следы с содержанием информации о преступнике, запрашивает дополнительную информацию и дает поручения оперативно-розыскным органам. В связи с этим след, содержащий информацию о личности преступника, представляет наибольший интерес для следователя.

Библиография

1. Буденко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // Lex Russica. 2016. № 4. С. 49-60.
2. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград: Волгоградская акад. МВД России, 2008. 401 с.
3. Жижилева А.А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы // Вопросы российской юстиции. 2019. № 3. С. 913-918.
4. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет: дис. ... канд. юрид. наук. М., 2018. 199 с.
5. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года // Министерство внутренних дел Российской Федерации. 2024. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 03.05.2024).
6. Крылов И.Ф. Криминалистическое учение о следах. Л.: Изд-во Ленинградского ун-та, 1976. 197 с.
7. Мазуров И.Е. Методика расследования хищений, совершенных с использованием интернет-технологий: автореф. дис. ... канд. юрид. наук. Ростов-на-Дону, 2017. 24 с.
8. Осипенко А.Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4. С. 31-34.
9. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Международной научно-практической конференции. Алматы, 2019. С. 6-8.
10. Себякин А.Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации: дис. ... канд. юрид. наук. М., 2021. 271 с.
11. Старостенко Н.И. Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук. Краснодар, 2023. 230 с.
12. Шебалин А.В. Расследование хищений средств сотовой связи: дис. ... канд. юрид. наук. Барнаул, 2010. 224 с.

Types of traces contributing to the identification of the person who committed the remote fraud

Andrei V. Kulaevskii

Postgraduate Student of the Department of Criminal Procedure
and Forensic Science,
Law Institute of the Altai State University,
656049, 68 Sotsialisticheskii ave., Barnaul, Russian Federation;
e-mail: andrei8888.98@mail.ru

Abstract

The article examines the traces left by the criminal when committing remote fraud. The author provides various classifications of crime traces formed in the information environment. The main digital traces left by the criminal at the time of the crime are indicated. Special attention is paid to the traces that make it possible to identify the person who committed the remote fraud. The conclusions are confirmed by examples from judicial and investigative practice. In addition to the digital traces available in science, the author identifies traces in the form of: information about incoming and outgoing traffic of a specific IP address stored by an Internet service provider or system administrator, as well as protocols for users on the Internet indicating connections. There are three groups of traces of remote fraud containing information about the person who committed it.

For citation

Kulaevskii A.V. (2024) Normativno-pravovye osnovaniya razvitiya programmy materinskogo (semeinogo) kapitala [Types of traces contributing to the identification of the person who committed the remote fraud]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (7A), pp. 449-456.

Keywords

Traces of crime, classification of traces, identification of the person who committed the crime, remote fraud, information environment.

References

1. Brief characteristics of the state of crime in the Russian Federation for January - December 2023 // Ministry of Internal Affairs of the Russian Federation. 2024. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (date of access: 03.05.2024).
2. Budenko O.S. Forensic and procedural aspects of conducting an inspection of mobile phones as part of a preliminary investigation // Lex Russica. 2016. No. 4. P. 49-60.
3. Kolycheva A.N. Recording of evidentiary information stored on Internet resources: dis. ... Cand. of Law. M., 2018. 199 p.
4. Krylov I.F. Forensic science of traces. L.: Publishing house of Leningrad University, 1976. 197 p.
5. Mazurov I.E. Methodology for investigating thefts committed using Internet technologies: author's abstract. dis. ... candidate of legal sciences. Rostov-on-Don, 2017. 24 p.
6. Osipenko A.L. Problems of involving electronic digital traces in criminal proceedings // Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia. 2009. No. 4. Pp. 31-34.
7. Rossinskaya E.R., Ryadovsky I.A. The concept of digital traces in forensic science // Aubakirov readings: materials of the International scientific and practical conference. Almaty, 2019. Pp. 6-8.

8. Sebyakin A.G. Tactics of using knowledge in the field of computer technology in order to obtain forensically significant information: diss. ... candidate of legal sciences. Moscow, 2021. 271 p.
9. Shebalin A.V. Investigation of thefts of cellular communications: diss. ... candidate of legal sciences. Barnaul, 2010. 224 p.
10. Starostenko N.I. The initial stage of the investigation of thefts committed using social engineering methods and information and telecommunication technologies: diss. ... candidate of legal sciences. Krasnodar, 2023. 230 p.
11. Vekhov V.B. Fundamentals of forensic science on the study and use of computer information and means of its processing: monograph. Volgograd: Volgograd Academy of the Ministry of Internal Affairs of Russia, 2008. 401 p.
12. Zhizhileva A.A. On some theoretical aspects of the use of the concepts of digital, electronic, virtual traces in forensics // Issues of Russian Justice. 2019. No. 3. P. 913-918.