

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

DOI: 10.17803/1994-1471.2022.144.11.140-148

Д. О. Буйнов*

Виды цифровых следов преступлений в сфере экономической деятельности и особенности их исследования экспертом

Аннотация. Цель данной статьи — выделить различные виды цифровых следов, несущих наиболее значимую информацию при расследовании преступлений в сфере экономической деятельности, определить особенности их исследования экспертом. Автором был поставлен ряд задач: проанализировать виды преступлений в сфере экономики и способы их совершения на предмет возможности образования цифровых следов в ходе осуществления данных правонарушений; выделить различные виды цифровых следов, характерных для каждого вида преступления; изучить судебную и экспертную практику по производству судебных экспертиз, объектом которых являются цифровые следы. Определены виды цифровых следов, имеющие наибольшую криминалистическую значимость при расследовании вышеуказанных преступлений, выявлены их характерные черты и особенности, рассмотрены отдельные аспекты экспертного исследования данных цифровых следов. Автор приходит к выводу, что наиболее распространенными цифровыми следами при расследовании экономических преступлений являются электронные бухгалтерские документы; информация, размещенная на сайте, используемая в преступной деятельности; данные сервера о регистрации сайта, о транзакции счетов. В связи с этим собирание цифровых следов наиболее целесообразно проводить: а) посредством изъятия материального носителя информации, содержащего электронные бухгалтерские документы; б) путем создания скриншота сайта, содержащего необходимую для расследования преступления информацию; в) путем направления запроса владельцу сервера, на ресурсах которого размещен сайт, используемый в преступной деятельности. Для экспертного исследования цифровых следов экономического содержания необходимо проведение комплекса судебных экспертиз.

Ключевые слова: цифровые следы; виды цифровых следов; образы цифровых следов; бухгалтерские документы; данные сервера; комплекс судебных экспертиз; судебная компьютерно-техническая экспертиза; судебные экономические экспертизы; преступления в сфере экономической деятельности; экспертное исследование цифровых следов.

Для цитирования: Буйнов Д. О. Виды цифровых следов преступлений в сфере экономической деятельности и особенности их исследования экспертом // Актуальные проблемы российского права. — 2022. — Т. 17. — № 11. — С. 140–148. — DOI: 10.17803/1994-1471.2022.144.11.140-148.

© Буйнов Д. О., 2022

* Буйнов Дмитрий Олегович, аспирант кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
bainovdmitrii@mail.ru

Types of Digital Traces of Crimes in the Field of Economic Activity and Features of their Study by an Expert

Dmitriy O. Buynov, Postgraduate Student, Department of Forensic Expertise, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
buinovdmitrii@mail.ru

Abstract. The purpose of this paper is to highlight various types of digital traces that carry the most significant information in the investigation of crimes in the field of economic activity, and to determine the features of their study by an expert. The author sets a number of tasks: to analyze the types of economic crimes and the methods of their commission for the possibility of the formation of digital traces in the course of the implementation of these offenses; to identify different types of digital traces specific to each type of crime; to study judicial and expert practice in the production of forensic examinations, the object of which are digital traces. The author identifies some types of digital traces that have the greatest forensic significance in the investigation of the above crimes, outlines their peculiarities and main features, and considers certain aspects of the expert study of these digital traces. The author concludes that the most common digital traces in the investigation of economic crimes are electronic accounting documents; information posted on a website used in criminal activities; server data on site registration and account transactions. In this regard, it is most expedient to collect digital traces: a) by seizing a material carrier of information containing electronic accounting documents; b) by creating a screenshot of the site containing the information necessary for the investigation of the crime; c) by sending a request to the owner of the server on whose resources the website used in criminal activities is located. For an expert study of digital traces of economic content, it is necessary to conduct a complex of forensic examinations.

Keywords: digital footprints; types of digital footprints; images of digital traces; accounting documents; server data; complex of forensic examinations; forensic computer-technical expertise; judicial economic examinations; crimes in the sphere of economic activity; expert study of digital footprints.

Cite as: Buynov DO. TVidy tsifrovyykh sledov prestupleniy v sfere ekonomicheskoy deyatel'nosti i osobennosti ikh issledovaniya ekspertom [Types of Digital Traces of Crimes in the Field of Economic Activity and Features of their Study by an Expert]. *Aktual'nye problemy rossijskogo prava*. 2022;17(11):140-148. DOI: 10.17803/1994-1471.2022.144.11.140-148. (In Russ., abstract in Eng.).

Развитие и внедрение современных информационно-телекоммуникационных технологий заметно изменило жизнь общества, предоставило новые возможности для развития государства, экономики, бизнеса и других сфер. Однако в силу своих отличительных особенностей цифровые технологии формируют и новые вызовы для правоохранительной системы. Преступники не могли не использовать последние тенденции для достижения собственных противоправных целей. Как уже не раз случалось, новейшие технологии были быстро освоены представителями преступности, что повлекло ее трансформацию вслед за быстро меняю-

щейся в сторону цифровизации сферой экономики и бизнеса. Согласно отчету ФКУ «Главный информационно-аналитический центр» МВД РФ о состоянии преступности в России за январь — ноябрь 2021 г. отмечается рост числа преступлений с использованием информационно-телекоммуникационных технологий на 7,1 % по сравнению с аналогичным периодом предыдущего года. При этом количество преступлений экономической направленности, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выросло на 51,1 %¹.

¹ Состояние преступности в Российской Федерации за январь — ноябрь 2021 г. // Главный информационно-аналитический центр МВД РФ. URL: <https://xn--b1aew.xn--p1ai/reports/item/27566319> (дата обращения: 12.01.2022).

Прежде чем приступить к определению видов цифровых следов, наиболее часто возникающих в ходе совершения преступлений в сфере экономической деятельности, необходимо сформулировать понятие цифрового следа.

Пожалуй, наиболее распространенным является подход к цифровому следу как совокупности информации, размещаемой пользователем о себе в сети Интернет². Данное определение можно назвать общеизвестным, ведь именно таким образом цифровой след понимается в повседневной жизни пользователей глобальной сети, и в первую очередь под такой информацией подразумеваются те сведения, которые пользователь оставляет в социальных сетях, мессенджерах, на почтовых серверах, в интернет-магазинах, иных используемых приложениях и на посещаемых сайтах.

Выделяются также активный и пассивный цифровые следы³. Согласно Концепции комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики, подготовленной на основе отчета Института законодательства и сравнительного правоведения при Правительстве РФ, выделяются два вида цифрового следа:

- 1) активный цифровой след, который формируется самим пользователем, который намеренно оставляет в информационных сетях различную информацию о себе;
- 2) пассивный цифровой след, образуемый данными, которые оставляются ненамеренно или вследствие работы программного обеспечения⁴.

Приведенные выше определения цифрового следа акцентируют внимание на данных, возникающих в ходе совершения действий в информационно-коммуникационных сетях. Однако, например, в рамках расследования преступлений в сфере экономической деятельности необходимо также исследование и различных электронных бухгалтерских документов, а кроме того, иных цифровых следов, которые могут быть образованы и без применения информационно-коммуникационных сетей.

Исходя из криминалистического понимания цифровых следов, наиболее подходящее определение, на наш взгляд, было дано Е. Р. Россинской и И. А. Рядовским, по мнению которых «цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи»⁵. Сходное определение было дано в монографии А. М. Багмета, В. В. Бычкова, С. Ю. Скобелина, Н. Н. Ильина: «Цифровой след — любая криминалистически значимая компьютерная информация, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»⁶. Данный подход не сужает сферу возможного возникновения цифровых следов до информационно-коммуникационных сетей, а предусматривает лишь компьютерную природу информации. Для целей криминалистики такая формулировка более оправдана, так как позволяет отнести к цифровым следам

² Бояркина Л. А., Бояркин В. В. Цифровой след и цифровая тень как производные персональных данных // Сборники конференций НИЦ «Социосфера». 2016. № 62. С. 79.

³ Никишин В. Д. Цифровые и речевые следы в аспекте обеспечения информационной (мировоззренческой) безопасности в интернет-среде // Судебная экспертиза. 2020. № 1. С. 132.

⁴ URL: https://webcache.googleusercontent.com/search?q=cache:ZUfngxYZ6X0J:https://sk.ru/documents/358/10.06.2020_%D0%9A%D0%9D%D0%9F%D0%A0_%D0%B4%D0%BE%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%81%D0%BB%D0%B5_%D0%A0%D0%93.pdf+&cd=1&hl=ru&ct=clnk&gl=nl (дата обращения: 16.01.2022).

⁵ Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). Алматы : Қазақстан Республикасы ИІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. С. 7.

⁶ Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н. Цифровые следы преступлений : монография. М. : Проспект, 2021. С. 168.

и те компьютерные файлы, которые были созданы, обработаны, изменены и без применения сети Интернет или других информационно-телекоммуникационных сетей.

Рассмотрим более подробно, каким образом тенденция цифровизации экономических отношений повлияла на изменение способов совершения преступления, а также на процесс доказывания при расследовании преступлений в сфере экономической деятельности. Бухгалтерский документооборот почти полностью (за исключением некоторых первичных учетных документов) переведен в электронный формат, организация и ведение бухучета на предприятии осуществляется автоматизированно с применением специальных компьютерных программ. Каждая экономическая операция находит свое отражение в базе данных, формируемой упомянутыми программами. Как следствие этого, при совершении преступлений в сфере экономической деятельности образуются различные цифровые следы, которые содержат доказательственную информацию, а именно: компьютерные файлы и базы данных, несущие сведения о характере и способах ведения предпринимательской деятельности, о фактах совершения отдельных транзакций и иных операций; количественные показатели, являющиеся основой для исчисления налогооблагаемой базы хозяйствующего субъекта, и т.д.

Использование различных интернет-ресурсов (интернет-магазинов, маркетплейсов, социальных сетей) для ведения предпринимательской деятельности только набирает обороты, чему способствуют ограничительные меры, введенные государствами в связи с пандемией COVID-19. Данный способ осуществления торговой и иной экономической деятельности используется и злоумышленниками, так как его применение дает определенную анонимность. Однако при осуществлении преступлений посредством создания интернет-сайта преступники оставляют цифровой след, информация о котором сохраняется на сервере сайта, а кроме того, данная информация может быть зафиксиро-

рована в образе, отображаемом в цифровом виде (скриншот).

Повсеместное распространение электронных денег и криптовалют в качестве средства платежа порождает новые сложности для правоохранительных органов вследствие таких особенностей криптовалюты, как высокий уровень анонимности, децентрализация финансовых сервисов, а также латентный характер использования физическими и юридическими лицами для проведения транзакций. Указанные свойства криптовалюты предопределили ее популярность у преступников для целей легализации (отмывания) доходов, полученных преступным путем. Тем не менее в таких случаях определенные цифровые следы, возникающие в ходе осуществления противоправной деятельности, позволяют получить криминалистически значимую информацию.

Вследствие данных процессов повышаются требования к квалификации судебных экспертов, специалистов-криминалистов правоохранительных органов, следователя. Возникает необходимость в разработке новых методик производства экспертного исследования, объектом которого является цифровой след, а также определение видов цифровых следов, несущих информацию о совершенном преступлении в сфере экономической деятельности, подробный анализ их характерных признаков и особенностей.

Приводятся множество классификаций цифровых следов, для чего применяются различные основания.

Е. Р. Россинская предлагает классификацию цифровых следов по месту хранения:

- 1) на отдельных носителях;
- 2) в компьютерных системах и сетях⁷.

В процессе собирания цифровых следов может возникнуть ситуация, когда зафиксировать и исследовать какую-либо компьютерную информацию можно будет только посредством создания и использования образа цифрового следа. Е. Р. Россинская предлагает выделять следующие виды образов цифровых следов:

⁷ Теория информационно-компьютерного обеспечения криминалистической деятельности / под ред. Е. Р. Россинской. М. : Проспект, 2022. С. 46.

- 1) образы, отображаемые в цифровом виде с помощью различных программных продуктов (например, скриншоты сайта);
- 2) образы, отображаемые на бумажных носителях (распечатанный на бумажном носителе образ документа)⁸.

Перечислим основные виды цифровых следов, представляющие наибольшую криминалистическую значимость при расследовании преступлений в сфере экономической деятельности:

- 1) электронные бухгалтерские и финансовые документы, электронные образы таких документов, образы документов, отображаемые на бумажных носителях;
- 2) данные интернет-ресурсов об организации торговли и ведения иной экономической деятельности преступниками (данные серверов, отображаемые в цифровом виде с помощью различных программных продуктов; данные о содержимом интернет-магазина (скриншоты) и т.д.);
- 3) данные соцсетей и мессенджеров, несущие информацию о совершении транзакций и иных экономических операций;
- 4) данные о цифровых финансовых активах.

При расследовании преступлений экономической направленности наибольший интерес представляют цифровые следы, содержащие информацию о совершении экономических операций. Это прежде всего электронные бухгалтерские документы и электронные образы таких документов. Стоит отметить, что в отличие от электронного документа, который создается в электронной форме без предварительного документирования на бумажном носителе и подписывается электронной подписью, электронный образ представляет собой переведенную в электронную форму с помощью средств сканирования копию документа, изготовленного на бумажном носителе, заверенную электронной подписью.

Обязательной характеристикой некоторых видов преступлений в сфере экономической

деятельности является причинение в результате противоправного деяния крупного ущерба гражданам, организациям или государству либо извлечение дохода в крупном размере, что позволяет квалифицировать деяние как уголовное преступление, а не административное правонарушение. В связи с этим при расследовании подобных преступлений требуется применение специальных бухгалтерских знаний для установления суммы дохода, полученного в результате незаконных действий.

Так, например, согласно приговору № 1-208/2019 от 28.06.2019 по делу № 1-208/2019 в рамках расследования дела о незаконном предпринимательстве была назначена судебная бухгалтерская экспертиза для определения суммы дохода, полученного в результате оказания услуг по теплоснабжению без получения лицензии на данную деятельность. Эксперту на исследование были представлены оптические диски CD-R, содержащие файлы формата «.xls» и другие с банковскими выписками по операциям и счетам общества с ограниченной ответственностью, отражающие получение денежных средств на счета общества в крупном размере. Эти бухгалтерские документы были предоставлены банком по запросу следствия⁹.

В России наиболее широко распространена система автоматизированного бухгалтерского учета «1С:Предприятие». При ее использовании для ведения бухгалтерского, налогового, операционного учета создается база данных в виде файла 1Cv8.CD, в котором хранятся различные сведения информационной системы, например конфигурация, база данных и т.д. Исследование файлов такого типа позволяет получить информацию об операциях, сформировать бухгалтерские регистры и установить интересующие следствие факты.

Так как этот компьютерный файл позволяет получить различную бухгалтерскую информацию, зачастую в ходе следствия, согласно ст. 201 УПК РФ¹⁰, назначается комплексная судебная

⁸ Теория информационно-компьютерного обеспечения криминалистической деятельности. С. 46.

⁹ Приговор Мичуринского городского суда (Тамбовская область) № 1-208/2019 от 28.06.2019 по делу № 1-208/2019 // URL: <https://sudact.ru/regular/doc/fm0rmXBU5kbT/> (дата обращения: 03.02.2022).

¹⁰ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СЗ РФ. 2001. № 52. Ст. 4921.

компьютерно-техническая экспертиза и судебная экономическая экспертиза. Однако есть ли необходимость в проведении комплексной экспертизы? Попробуем рассмотреть этот вопрос на примере расследования налогового преступления, когда на экспертизу представлен файл базы данных системы автоматического бухгалтерского учета.

При расследовании налоговых преступлений следствие интересуется размером уплаченного юридическим лицом в бюджет налога. Перед экспертом-экономистом стоит задача определить сумму налога, которую должно было заплатить предприятие за определенный период, и сумму, которую оно фактически заплатило. Для расчета налогооблагаемой базы, исчисляемой согласно налоговому законодательству, эксперту необходимо исследовать бухгалтерские документы — бухгалтерские регистры и первичные учетные документы, которые и являются объектами налоговой экспертизы¹¹.

Эксперт-экономист может сформировать эти документы, которые содержатся в базе данных. Однако не всегда он способен самостоятельно получить нужные документы. Кроме того, следствие могут интересовать различные факты видоизменения базы данных, факты изменения конфигурации базы данных сотрудниками предприятия для целей бухгалтерского учета. По этой причине следствие назначает комплексную судебную компьютерно-техническую и судебную налоговую экспертизу.

Насколько обоснованно назначение именно комплексной экспертизы? Ведь ее отличительной особенностью является невозможность решения вопроса без одновременного совместного участия экспертов различных родов судебных экспертиз в написании заключения и формулировании общего вывода¹². В рассматриваемом случае отсутствует задача, решение которой требовало бы одновременного применения специальных знаний из различных обла-

стей. При производстве судебной компьютерно-технической экспертизы с целью установления фактов видоизменения базы данных, конфигурации и т.д. нет необходимости в специальных экономических знаниях. При исследовании же бухгалтерских документов с целью проверки правильности исчисления налога нет необходимости в участии эксперта в области судебной компьютерно-технической экспертизы. Возможно, потребуется лишь обеспечить доступ к базе данных эксперта-экономиста и представление бухгалтерских данных в читаемом виде, предотвратить случайное изменение файла базы данных.

Исходя из этого, можно прийти к выводу, что назначение комплексной экспертизы здесь неоправданно. Более подходящим решением было бы назначить комплекс экспертиз, в который входила бы судебная компьютерно-техническая и судебная налоговая экспертизы. Если же проведение специального исследования в сфере компьютерно-технической экспертизы необязательно и у следствия нет вопросов, разрешение которых требовало бы соответствующих специальных знаний, а требуется только предоставление доступа эксперту-экономисту к базе данных, а также предотвращение случайных изменений файла базы данных, то целесообразнее назначить судебную налоговую экспертизу и обеспечить участие специалиста, обладающего специальными знаниями, необходимыми для представления бухгалтерских данных в читаемом виде.

Стоит также рассмотреть некоторые другие особенности цифровых следов, исследуемых в рамках уголовного судопроизводства дел о незаконном предпринимательстве. Особого внимания заслуживают изъятие и исследование цифровых следов по делам об организации и осуществлении предпринимательской деятельности без регистрации или без лицензии посредством создания интернет-магазинов. При

¹¹ Голикова В. В. Предмет, объекты и задачи судебной налоговой экспертизы расчетов с бюджетом по налогу на добавленную стоимость // Вестник Университета имени О.Е. Кутафина (МГЮА). 2018. № 7. С. 53.

¹² Россинская Е. Р. Методологические и правовые проблемы комплексных судебных экспертиз в условиях реформирования законодательства о судебно-экспертной деятельности // Вестник Московского университета МВД России. 2014. № 6. С. 15.

этом размещенная на веб-сайте информация, необходимая для доказывания факта ведения торговой деятельности, может быть зафиксирована и изъята посредством создания снимков экрана (скриншотов). Возможность такого изъятия представлена следующим примером из практики. Из приговора Индустриального районного суда г. Перми № 1-455/2014 455/14 от 10.11.2014 по делу № 1-455/2014¹³ следует, что гражданин осуществлял реализацию продукции (семена конопли) без регистрации юридического лица и без регистрации в качестве индивидуального предпринимателя в особо крупном размере. Продукция реализовывалась с помощью веб-сайта, на котором была размещена ее реклама, а также элементы интерфейса (рабочие окна, кнопки, графы для ввода данных), предназначенные для оформления заказа. Эта текстовая и графическая информация была зафиксирована посредством создания снимков экрана.

Еще одним преступлением в сфере экономической деятельности, которое может совершаться посредством создания интернет-магазина, является осуществление незаконной банковской деятельности. Указанная деятельность включает в себя различные банковские операции, в том числе обмен национальных и цифровых валют, переводы денежных средств (в том числе электронных) без открытия банковских счетов и другие виды операций. В ходе уголовного судопроизводства данной категории дел экспертное исследование цифровых следов также весьма актуально. Так, например, в ходе следствия могут быть исследованы различные устройства и носители, содержащие в цифровом формате сведения, указывающие на ведение незаконной банковской деятельности. Примером может послужить уголовное дело № 1-416/2017. Согласно приговору Свердловского районного суда г. Костромы № 1-416/2017 1-9/2018 от 16.07.2018¹⁴ по указанному делу, в ходе следствия были изъяты мобильные телефоны, SIM-карты, ноутбуки. В ходе судебной компьютерно-техниче-

ской экспертизы на SIM-картах и во внутренней памяти мобильных телефонов были обнаружены аудиофайлы входящих звонков, сведения о доступе к интернет-ресурсам, в том числе об обмене сообщениями между абонентами при помощи программных продуктов, а также СМС-сообщениями (среди которых входящие сообщения от абонентов об осуществлении входа в интернет-банк, о поступлении, списании и переводе денежных средств в различных суммах, пополнении карты, коды доступа), о платежных системах и финансово-кредитных организациях. При осмотре накопителя на жестких магнитных дисках изъятого ноутбука экспертом были обнаружены сведения об обмене сообщениями между клиентами за год, сводящиеся к обмену титульных знаков между собой.

Экспертное исследование цифровых следов зачастую необходимо и в ходе уголовного судопроизводства дел о легализации денежных средств или иного имущества, приобретенного преступным путем. Желая придать правомерный вид владению, пользованию и распоряжению денежными средствами, приобретенными в результате совершения преступления, правонарушители прибегают к совершению финансовых операций с использованием электронных платежных систем и криптовалюты.

Определение криптовалюты (цифровой валюты) дано в ч. 3 ст. 1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»¹⁵, вступившего в силу с 1 января 2021 г., в соответствии с которой цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в

¹³ URL: <https://sudact.ru/regular/doc/mljgZYf1HSV/> (дата обращения: 03.02.2022).

¹⁴ URL: <https://sudact.ru/regular/doc/BpRtLg3cn3ZW/> (дата обращения: 03.02.2022).

¹⁵ СЗ РФ. 2020. № 31. Ст. 5018.

отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам.

В случае если сервер компании, предоставляющей услуги электронно-платежной системы, расположен на территории Российской Федерации, то информация о транзакциях счетов может быть предоставлена по запросу следствия, после чего направлена на экспертное исследование для определения общей суммы финансовых операций по легализации денежных средств, приобретенных преступным путем.

Определение видов цифровых следов при расследовании различных преступлений в сфере экономической деятельности необходимо как для формирования методики экспертного исследования этих следов, так и для разработки теоретических основ учения о цифровых следах. Можно утверждать, что к цифровым следам необходимо относить не только данные, возникающие в ходе совершения действий в информационно-

коммуникационных сетях, но и вообще любую криминалистически значимую компьютерную информацию, в том числе и созданную без применения подобных сетей. Наибольший интерес для расследования экономических преступлений представляют электронные бухгалтерские документы, информация на сайте, используемом в преступной деятельности, данные сервера о регистрации сайта, о транзакции счетов.

Собирание цифровых следов наиболее целесообразно проводить посредством изъятия материального носителя информации, содержащего электронные бухгалтерские документы, путем создания скриншота сайта, содержащего необходимую для расследования преступления информацию; путем запроса владельцу сервера, на ресурсах которого размещен сайт, использующийся в преступной деятельности.

Для экспертного исследования цифровых следов необходимо назначение компьютерно-технической экспертизы, кроме того, при исследовании электронных бухгалтерских документов требуется назначение экономической экспертизы. Причем целесообразно проведение комплекса различных экспертиз, а не назначение комплексной судебной компьютерно-технической и экономической экспертизы.

БИБЛИОГРАФИЯ

1. Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н. Цифровые следы преступлений : монография / Следственный комитет Российской Федерации ; Московская академия Следственного комитета Российской Федерации. — М. : Проспект, 2021. — 244 с.
2. Бояркина Л. А., Бояркин В. В. Цифровой след и цифровая тень как производные персональных данных // Сборники конференций НИЦ «Социосфера». — 2016. — № 62. — С. 78–81.
3. Голикова В. В. Предмет, объекты и задачи судебной налоговой экспертизы расчетов с бюджетом по налогу на добавленную стоимость // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2018. — № 7. — С. 53–60.
4. Никишин В. Д. Цифровые и речевые следы в аспекте обеспечения информационной (мировоззренческой) безопасности в интернет-среде // Судебная экспертиза. — 2020. — № 1 (61). — С. 131–139.
5. Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). — Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. — С. 6–8.
6. Россинская Е. Р. Методологические и правовые проблемы комплексных судебных экспертиз в условиях реформирования законодательства о судебно-экспертной деятельности // Вестник Московского университета МВД России. — 2014. — № 6. — С. 12–18.

7. Теория информационно-компьютерного обеспечения криминалистической деятельности / под ред. Е. Р. Россинской. — М. : Проспект, 2022. — 256 с.

Материал поступил в редакцию 26 марта 2022 г.

REFERENCES (TRANSLITERATION)

1. Bagmet A. M., Bychkov V. V., Skobelin S. Yu., Ilin N. N. Tsifrovye sledy prestupleniy: monografiya / Sledstvennyy komitet Rossiyskoy Federatsii; Moskovskaya akademiya Sledstvennogo komiteta Rossiyskoy Federatsii. — M.: Prospekt, 2021. — 244 s.
2. Boyarkina L. A., Boyarkin V. V. Tsifrovoy sled i tsifrovaya ten kak proizvodnye personalnykh dannykh // Sborniki konferentsiy NITs «Sotsiosfera». — 2016. — № 62. — S. 78–81.
3. Golikova V. V. Predmet, obekty i zadachi sudebnoy nalogovoy ekspertizy raschetov s byudzhетom po nalogu na dobavlenuyu stoimost // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). — 2018. — № 7. — S. 53–60.
4. Nikishin V. D. Tsifrovye i rechevye sledy v aspekte obespecheniya informatsionnoy (mirovovzrencheskoy) bezopasnosti v internet-srede // Sudebnaya ekspertiza. — 2020. — № 1 (61). — S. 131–139.
5. Rossinskaya E. R., Ryadovskiy I. A. Kontsepsiya tsifrovyykh sledov v kriminalistike // Aubakirovskie chteniya: materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii (19 fevralya 2019 g.). — Almaty: Qazaqstan Respublikasy IIM M. Esbolatov atyndary Almaty akademiya synuң FZzhRBZhҮB, 2019. — S. 6–8.
6. Rossinskaya E. R. Metodologicheskie i pravovye problemy kompleksnykh sudebnykh ekspertiz v usloviyakh reformirovaniya zakonodatelstva o sudebno-ekspertnoy deyatel'nosti // Vestnik Moskovskogo universiteta MVD Rossii. — 2014. — № 6. — S. 12–18.
7. Teoriya informatsionno-kompyuternogo obespecheniya kriminalisticheskoy deyatel'nosti / pod red. E. R. Rossinskoy. — M.: Prospekt, 2022. — 256 s.