Научная статья
УДК 343.985

ПОНЯТИЕ И ВИДЫ ЦИФРОВЫХ СЛЕДОВ, ИХ ЗНАЧЕНИЕ В РАССЛЕДОВАНИИ ВЗЯТОЧНИЧЕСТВА

Елена Викторовна Христинина[1,2]
[1] Омский государственный технический университет, Омск, Россия,
[2] Сибирский институт бизнеса и информационных технологий, Омск, Россия,
elena.nikitina83@mail.ru

Аннотация. Актуальность настоящей работы обусловлена научной проблемой, связанной с тем, что при раскрытии и расследовании взяточничества, где преступник применяет информационно-телекоммуникационные технологии, могут возникать определенные сложности, связанные с обнаружением и изъятием цифровых следов, которые характеризуют механизм коррупционного преступления. Отмечается, что в настоящее время отсутствует комплексное исследование, посвященное выявлению цифровых следов при расследовании взяточничества. В научной статье вынесено предложение о введении криминалистического учета электронных следов преступления, который улучшит взаимодействие между следователями, дознавателями, находящимися на территории разных субъектов, если одно и то же лицо совершило несколько преступлений. Эффективность расследования взяточничества с использованием компьютерно-информационных технологий напрямую зависит от правильной работы по обнаружению, изъятию, исследованию цифровых следов. Неоценима роль хорошо подготовленного специалиста, который окажет помощь в фиксации и изъятии цифровых следов.

Ключевые слова: взяточничество, цифровые следы, информационно-телекоммуникационные технологии, расследование преступлений, следственные действия, следователь, взяткодатель, взяткополучатель, цифровизация, блокчейн-технологии, криптовалюта.

Для цитирования: Христинина Е. В. Понятие и виды цифровых следов, их значение в расследовании взяточничества // Вестник Уфимского юридического института МВД России. 2025. № 2 (108). С. 127–135.

Original article

THE CONCEPT AND TYPES OF DIGITAL TRACES, THEIR SIGNIFICANCE IN THE INVESTIGATION OF BRIBERY

Elena V. Khristinina[1,2]
[1] Omsk State Technical University, Omsk, Russia,
[2] Siberian Institute of Business and Information Technology, Omsk, Russia,
elena.nikitina83@mail.ru

Abstract. The relevance of this work is due to the scientific problem associated with the fact that in the disclosure and investigation of bribery, where the criminal uses information and telecommunication technologies, certain difficulties may arise related to the detection and seizure of digital traces that characterize the mechanism of a corruption crime. It is noted that there is currently no comprehensive study dedicated to the identification of digital traces in the investigation of bribery. The scientific article proposes the introduction of forensic accounting of electronic traces of a crime, which will improve the interaction between investigators and interrogators located on the territory of different subjects if the same person has committed several crimes. The effectiveness of the investigation of bribery using computer and information technologies directly depends on the correct work on the detection, seizure, and investigation of digital traces. The role of a well-trained specialist who will assist in fixing and removing digital traces is invaluable.

Keywords: bribery, digital traces, information and telecommunication technologies, crime investigation, investigative actions, investigator, bribe taker, bribe recipient, digitalization, blockchain technologies, cryptocurrency.

For citation: Khristinina E. V. The concept and types of digital traces, their significance in the investigation of bribery // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2025. № 2 (108). P. 127–135. (In Russ.)

Введение

Следует отметить, что до сих пор являются актуальными вопросы, связанные с расследованием взяточничества, так как данный вид преступления является распространенным. Актуальность коррупционного преступления обусловлена тем, что оно нарушает работу государственных органов, снижает авторитет власти перед населением, нарушает права граждан и в итоге причиняет существенный экономический ущерб государству.

Необходимо обратиться к официальной статистике, где указаны следующие данные. За январь – август 2024 г. правоохранительными органами были выявлены преступления коррупционной направленности в количестве 28542 случаев, из них 16914 преступлений связано со взяточничеством, а именно: 5980 случаев – получение взятки, 4887 случаев – дача взятки, 1896 случаев – посредничество во взяточничестве и, наконец, 4151 случай – мелкое взяточничество. Статистика подтверждает тезис о распространенности взяточничества как вида преступлений.

Цифровизация общества приводит к тому, что преступные коррупционные посягательства совершаются с использованием информационно-телекоммуникационных технологий. Следует обратиться к официальным статистическим сведениям ГИАЦ МВД России, в которых указано, что в период с января по август 2024 г. было выявлено 500389 случаев преступлений, совершенных с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации. Более того, статистические сведения говорят о росте анализируемых преступлений на 16,5 % по сравнению с предыдущим годом, их удельный вес за период с января по август 2023 года существенно увеличился до 38,4 %[1]. Следовательно, в настоящее время назрела необходимость в проведении комплексного исследования, посвященного выявлению цифровых следов при расследовании взяточничества.

Методы исследования

Методологическая основа научного исследования основывается на общенаучных и специальных методах научного познания. Методика научного исследования основана на рассмотрении правовых норм Уголовного кодекса Российской Федерации, Уголовно-процессуального кодекса Российской Федерации, научных трудов, материалов следственной и судебной практики по теме проводимого научного исследования.

Результаты исследования

Следует указать, что отдельные виды взяточничества могут совершаться с применением средств удаленного доступа, в результате которого могут появляться цифровые следы преступления. Причинами совершения взяточничества с использованием информационно-телекоммуникационных технологий могут выступать информатизация всех систем, применение электронных денег в качестве предмета взятки, усложняющих процесс изобличения преступника. Кроме того, средством для передачи электронных денег может выступать электронная почта, принадлежащая взяткополучателю, с помощью которой последний узнает код, на основании которого можно обналичить денежные средства. Отдельный интерес представляет использование взяткополучателем

[1] Статистика // МВД России: сайт. URL: https://мвд.рф/reports/item/55225633/ (дата обращения: 14.10.2024).

определенного предмета преступления – криптовалюты. Ее появление было обусловлено развитием блокчейн-технологии для того, чтобы электронная валюта была не контролируема государством.

К сожалению, законодатель в статью 290 УК РФ в качестве предмета взятки включил лишь деньги, ценные бумаги, иное имущество, незаконное оказание услуг имущественного характера, иные имущественные права. Криптовалюта в виде биткоина в качестве предмета преступления не упоминается.

Однако следует обратиться к Постановлению Пленума Верховного Суда Российской Федерации № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях»[1]. В пункте 10 вышеуказанного постановления говорится о том, что получение взятки считается оконченным преступным деянием с момента зачисления электронных денег с согласия должностного лица на указанный им банковский счет, «электронный кошелек». Тем самым законодатель косвенно относит к предмету взятки криптовалюту.

В настоящее время законодатель ввел понятие криптовалюты в ч. 3 ст. 1 Федерального закона от 31 июля 2020 г. № 259 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[2]. Согласно закону 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.

Таким образом, использование информационных технологий при получении взятки влечет изменение механизма преступления за счет отсутствия прямого контакта между взяткодателем и взяткополучателем, в результате чего появляется термин «дистанционное взяточничество». В результате вышеизложенного появляются сложности в расследовании преступления и установлении виновного лица. К примеру, эти сложности обусловлены тем, что IP-адреса, серверы и ресурсы, с которых совершаются преступные деяния, могут находиться вне юрисдикции нашего государства. Следовательно, основная задача органов расследования своевременно получать криминалистически важную информацию о совершении дистанционных взяточничеств из анализа цифровых следов преступления.

Констатируется, что проблемой изучения цифровых следов, возникающих при совершении различных преступлений, занимаются различные ученые. В научной литературе существует множество определений понятия «виртуальные следы» (В. А. Мещеряков, В. Ю. Агибалов, А. Б. Смушкин и др.), электронно-цифровые следы (В. Б. Вехов и др.), цифровые следы» (Е. Р. Россинская, И. А. Рядовский, М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин и др.).

В. А. Мещеряков справедливо указывает, что виртуальные следы представляют собой «любые изменения состояния автоматизированной информационной системы («кибернетического пространства»), связанные с событием преступления и зафиксированные в виде компьютерной информации на материальном носителе, в том числе электромагнитном поле» [1, с. 74]. Исходя из представленного определения, он выделяет особенные свойства виртуального следа, благодаря которому следы могут изымать, исследоваться следственными органами при расследовании многих преступлений.

[1] О судебной практике о взяточничестве и об иных коррупционных преступлениях : постановление Пленума Верховного Суда Российской Федерации от 9 июля 2013 г. № 24 // Бюллетень Верховного Суда Российской Федерации. 2013. № 9.

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : федеральный закон от 31 июля 2020 г. № 259ФЗ (в ред. от 11 марта 2024 г. № 45-ФЗ) // Собрание законодательства Российской Федерации. 2020. № 31 (часть I), ст. 5018.

Позиция автора обусловлена тем, что «виртуальные следы» занимают промежуточное межу между видами следов: идеальными и материальными. В. А. Мещеряков объясняет необходимость выделения таких следов тем, что они содержатся на материальном носителе, однако их обнаружение и изъятие возможно только с помощью программно-технических средств, так как по-другому они не могут быть восприняты.

Представляется, что включение «виртуальных следов» в состав материальных следов не является возможным, так как следы содержат субъективную составляющую, зависящую от способа их считывания, и не имеют прочной связи с устройством, которое записывает информацию. Они также являются неустойчивыми, что делает их ближе к идеальным следам. Однако они не могут быть классифицированы как идеальные следы, так как хранятся на материальных объектах, а не в человеческой памяти.

В. Ю. Агибалов отождествляет термин «цифровой след» с термином «след-модель», включая в его содержание «упорядоченную совокупность электронных цифровых данных, отражающих абстрактную модель и параметры реального объекта, относящегося к расследуемому уголовному делу» [2, с. 353]. Позиция автора основана на том, что при использовании цифровой записи звука или изображения сохраняется абстрактная математическая модель исходного объекта, а не сам объект или его полное отражение. Эта модель определяется видом математической модели и ее параметрами. Таким образом, при цифровой записи информации на материальный носитель фиксируется последовательность чисел, которая представляет параметры абстрактной модели.

А. Б. Смушкин изучает виртуальные следы с позиции совершения определенных действий, определяя, что это «следы совершения действий: включения, создания, открывания, активации, внесения изменений, удаления в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей» [3, с. 43].

Полагаем, что термин «виртуальные следы» сложно использовать при расследовании преступлений, поскольку он уже активно применяется в квантовой теории поля в ходе описания квантовых частиц и относится к виртуальной реальности. В контексте расследования преступлений, где требуется сбор фактических доказательств и установление конкретных фактов, использование термина «виртуальные следы» может вызывать определенную путаницу.

Профессор В. Б. Вехов рассматривает понятие «электронно-цифровой след» как «любую криминалистически значимую компьютерную информацию, зафиксированную на материальном носителе с помощью электромагнитных взаимодействий либо передающуюся по каналам связи посредством электромагнитных сигналов» [4, с. 27; 5, с. 11].

С теоретической и практической стороны данную точку зрения автора считаем логичной, так как данный термин обозначает двойственную природу следов: электронные следы, которые могут оставаться на различных материальных носителях, и цифровые следы, которые представлены в виде цифрового кода или изменений, зафиксированных в цифровом коде в памяти электронных устройств. Такое название позволяет более точно говорить, о каких именно следах идет речь, а также учитывать их электронную и цифровую природу.

Однако полагаем, правильнее применять понятие «цифровой след» при расследовании преступлений. Коллектив авторов (А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин) в научных исследованиях применяют термин «цифровые следы», под которым понимают «любую криминалистически значимую компьютерную информацию, содержащую сведения (сообщения, данные), представленную в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [6, с. 130].

С криминалистической точки зрения, как справедливо считают Е. Р. Россинская и И. А. Рядовский, следует рассматривать цифровой след как «криминалистически значимую компьютерную информацию о

событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [7, с. 7]. Представляется, что данная точка зрения является правильной, потому что в авторском определении учитывают особенности цифровых следов как материальных объектов. Бесспорно, цифровые следы остаются на различных материальных объектах в результате определенных событий. Это указывает на важность термина «цифровой след» для более точного описания и понимания их природы.

Кроме того, данная научная позиция авторов учитывает технологические особенности формирования следов, которые возникают в результате использования информационных технологий, так как для их анализа и преобразования в необходимую форму для возможности восприятия применяются информационные технологии. Таким образом, определение, предложенное авторами, учитывает важные аспекты, которые помогают правильно интерпретировать и использовать цифровые следы в качестве доказательств в расследовании преступлений.

Цифровые следы можно разделить по различным основаниям. Следует рассмотреть различные классификации, представленные учеными (А. Г. Волеводз, В. Б. Вехов, В. А. Мещеряков, А. Б. Смушкин, Е. Р. Россинская).

А. Г. Волеводз выделяет классификацию цифровых следов исходя из места нахождения цифрового носителя: следы, отображенные на жестком диске, на компьютере, на устройствах периферийного оборудования, на устройствах связи, следы в проводных, радиооптических и других электромагнитных системах [8, с. 35].

Классификация, представленная А. Г. Волеводз, имеет ряд недостатков в связи с постоянным развитием технологий и изменением носителей цифровых данных. Ранее используемые носители, такие как магнитные ленты и дискеты, уже утратили актуальность и перестали использоваться. Следовательно, данная классификация является неполной, поскольку в ней новые технологии и носители данных были упущены или недостаточно учтены. Необходимо постоянно обновлять и адаптировать классификацию, чтобы учитывать новые технологические разработки и носители цифровых следов.

Интересной является точка зрения В. А. Мещерякова, полагающего, что «виртуальные следы» нельзя отнести к материальным и к идеальным преступным следам, а следует их выделять в обособленную группу, имеющую свою специфику [9, с. 28].

А. Б. Смушкин предлагает совершенно другой научный подход к классификации виртуальных следов, основанный на событиях и действиях, происходящих в памяти компьютера при его использовании. Например, следы могут быть классифицированы в зависимости от операций, выполняемых с содержимым памяти компьютера, таких как включение, выключение и различные операции с данными. Также возможна классификация следов на основе действий с наиболее важными программами, необходимыми для работы компьютера [3, с. 43]. Такой подход позволяет более точно описывать и классифицировать цифровые следы, учитывая разнообразие действий и событий, которые могут возникать в ходе использования компьютерных технологий.

Е. Р. Россинская классифицирует цифровые следы на две группы исходя из места их хранения: следы, находящиеся на отдельных носителях информации, и следы, содержащиеся в компьютере или информационной системе [10, с. 46]. На практике при исследовании цифровых следов в ходе расследования взяточничества органы расследования в некоторых ситуациях можно получить только образ цифрового следа. Именно поэтому Е. Р. Россинская указывает, что образы цифрового следа также можно разделить на две самостоятельные группы: образы цифрового следа, возникающие в ходе использования компьютерных программ, и образы цифрового следа, появляющиеся на бумажном носителе [11, с. 35]. Данная точка зрения автора является справедливой, поскольку образы цифрового следа, действительно,

могут быть представлены не только в электронном формате, но и на бумажных носителях, тем самым проявляется двуединство природы цифрового следа.

При расследовании преступлений, связанных с взяточничеством, следователь придает особое значение изучению цифровых следов, которые оставляют преступники при использовании различных цифровых устройств, таких как компьютеры, смартфоны. В этих устройствах может содержаться искомая информация, представленная в виде следов, указывающих на подготовку и совершение преступления. Поэтому для расширения доказательной базы в уголовном деле следователю необходимо тщательно изучить все электронные устройства, используемые участниками преступления, с целью обнаружения такой информации [12, с. 78].

Проанализировав эмпирические данные, полученные путем анализа уголовных дел, связанных с расследованием взяточничества, следует выделить разновидности цифровых следов, которые необходимо изучать следственным органам для получения криминалистически значимой информации:

1) электронную финансовую документацию, содержащую цифровые следы относительно проведенных банковских операций по переводам денежных средств;

2) цифровые следы, находящиеся в социальных сетях и мессенджерах, содержащие переписку взяткодателя с взяткополучателем относительно совершения преступления;

3) информацию об имеющихся цифровых активах преступника;

4) сведения о средствах связи, применяемых взяткодателем и взяткополучателем в ходе общения по поводу передачи-получения предмета взятки;

5) сведения об используемых преступниками интернет-ресурсах (доменные адреса web-сайтов, IP-адреса, адреса электронной почты);

6) сведения о банковских картах, «электронных кошельках», применяемые при переводе незаконного вознаграждения взяткодателем взяткополучателю.

Представляется, что необходимо при расследовании взяточничества тщательно выявлять и в последующем изучать цифровые следы, содержащиеся в сети Интернет, в средствах мобильной связи, компьютере и иных средствах информации при производстве следственных действий. Специфика цифровых следов обусловлена тем, что они могут легко уничтожаться, изменяться и распространяться по различным каналам связи, поэтому важная задача органов расследования – оперативно проводить необходимые следственные действия, такие как осмотр места происшествия, обыск, выемка.

Следует отметить, что обнаружение, фиксация и изъятие цифровых следов – это результат тщательной подготовки правоохранительных органов к производству следственного действия. При этом учитываются характер совершенного преступного деяния, ход действий следственно-оперативной группы, работа специалиста с цифровыми следами.

Для обнаружения и изъятия таких цифровых следов в цифровом пространстве применяются специализированные технические средства, включая программное и аппаратное обеспечение. Одним из наиболее используемых программно-аппаратных комплексов для извлечения и анализа данных с мобильных устройств является «Мобильный криминалист». При помощи этого инструмента возможно создание физических и логических образов устройств, а также извлечение и расшифровка данных, включая удаленную информацию, с мобильных телефонов, смартфонов, планшетов и других персональных устройств. Программа разработана в России и является основным инструментом для проведения исследований в данной области.

Другим программным комплексом выступает UFED Touch, разработанный в Израиле, который предназначен для проведения криминалистических исследований. Он предоставляет специалистам возможность извлекать, декодировать и анализировать сведения, полученные с различных моделей мобильных средств связи. С помощью

UFED Touch криминалисты могут использовать эту информацию в судебных процессах.

Программная система XRY, производимая в Швейцарии, является способом для считывания и анализа информации с мобильных телефонов и сим-карт. Она позволяет получить различные данные, такие как контакты на сим-карте и в памяти телефона, историю звонков, смс-сообщения, данные из календаря, списки дел и заметок, а также медиафайлы, сохраненные в памяти телефона. С помощью XRY можно извлекать удаленную информацию с сим-карты, а также определить идентификационный номер телефона (IMEI) и индивидуальный номер абонента (IMSI).

Кроме того, существует несколько программных продуктов, которые предназначены для восстановления удаленной, модифицированной или поврежденной цифровой информации с материальных носителей. Такими программными обеспечениями являются RStudio, EASYUS File Recovery, Ontrack EasyRecovery и другие, которые предоставляют возможность восстановить потерянные файлы с различных носителей, таких как жесткие диски, флэш-накопители, SD-карты и т. д. Программы используют различные алгоритмы и методы для поиска и восстановления данных, давая пользователям широкий спектр инструментов для восстановления утраченной информации.

На практике также может применяться «ОПТИК-2». Это специализированное устройство для обнаружения скрытых видеокамер какого-либо объекта, предназначенное для отслеживания пути записи видеофайлов. Криминалисты могут использовать это устройство для изъятия интересующих видеоданных.

Важно отметить, что приведенные программные комплексы хорошо дополняют друг друга. Например, если программа UFED Touch не может извлечь определенную информацию, ее можно получить с помощью программы «Мобильный криминалист» и наоборот. Таким образом, посредством изучения извлеченной информации с различных программных средств криминалисты могут получить более полное представление о цифровом следе при расследовании преступления.

Из-за сложности работы с цифровыми следами следователю надлежит приглашать хорошо подготовленного специалиста, который окажет помощь в фиксации и изъятии цифровых следов. Конечно, на практике у следователя может возникать проблема относительно выбора специалиста, обладающего профессионализмом по работе с цифровыми следами. Именно поэтому справедливой является точка зрения А. И. Семикаленовой и И. А. Рядовского, считающих, что при проведении таких следственных действий, как осмотр, обыск и выемка, где могут быть обнаружены и в последующем изъяты цифровые следы, необходимо обеспечить обязательное участие специалистов широкого профиля в сфере информационных технологий [13, с. 178].

Цифровой след, изъятый в ходе производства следственного действия, в последующем будет являться объектом исследования при назначении и проведении таких компьютерных экспертиз, как аппаратно-компьютерная, программно-компьютерная, информационно-компьютерная экспертиза (данных), компьютерно-сетевая экспертиза.

Заключение

Сложность поиска эффективных мер по собиранию, обработке, систематизации и поиску цифровых следов в целях раскрытия и расследования взяточничества обусловлена отсутствием отдельной методики, посвященной выявлению, фиксации и исследованию цифровых следов. Следовательно, отсутствие необходимых знаний у следователя в области информационных технологий может привести к ситуации, когда криминалистически значимая информация, содержащаяся в цифровых следах, может быть утрачена, а это может отразиться на качестве расследования взяточничества [14, с. 35]. В связи с вышесказанным следует внести предложение о повышении квалификации следователей, дознавателей, опера-

тивных работников по работе с цифровыми следами, обнаруженными на месте преступления при расследовании взяточничества [15, с. 45].

Представляется, что назрела необходимость не только тщательно изучать цифровые следы, но создать криминалистический учет и последующую идентификацию на этой основе электронно-цифрового следа. Создание криминалистического учета электронных следов улучшит взаимодействие между следователями из разных субъектов, если одни и те же преступники совершили преступные деяния.

Таким образом, следует сделать вывод о том, что эффективность расследования взяточничества с использованием компьютерно-информационных технологий напрямую зависима от работы следственных органов, направленной на обнаружение, изъятие, исследование цифровых следов. Важнейшую роль в ходе проведения таких следственных действий, как осмотр, обыск и выемка, играет специалист широкого профиля в сфере информационных технологий, который поможет следственным органам правильно зафиксировать, а в последующем и изъять цифровой след преступления.

СПИСОК ИСТОЧНИКОВ

1. Мещеряков В. А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: Воронежский государственный университет, 2001. 255 с.

2. Агибалов В. Ю. Криминалистическая сущность виртуальных следов // Вестник Воронежского государственного университета. Серия: Право. 2009. № 2. С. 350–355.

3. Смушкин А. Б. Виртуальные следы в криминалистике // Законность. 2012. Вып. 8. С. 43–45.

4. Вехов В. Б. Основы криминалистического учения об исследования и использовании компьютерной информации и средств ее обработки. Волгоград: Волгоградская академия МВД России, 2008. 404 с.

5. Вехов В. Б. Электронные следы в системе криминалистики // Судебная экспертиза. 2016. № 2. С. 10–18.

6. Багмет А. М. Цифровые следы преступлений: монография. М.: Проспект, 2021. 168 с.

7. Россинская Е. Р. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы международной научно-практической конференции. Алматы, 2019. С. 6–9.

8. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.

9. Мещеряков В. А. Виртуальные следы под «скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1. С. 28–33.

10. Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. М.: Проспект, 2022. 256 с.

11. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник университета имени О. Е. Кутафина (МГЮА). 2019. № 5. С. 35–36.

12. Бояркина Л. А. Цифровой след и цифровая тень как производные персональных данных // Сборники конференций НИЦ «Социосфера». 2016. № 62. С. 78–81.

13. Семикаленова А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 178–184.

14. Зуев С. В. Основы теории электронных доказательств: монография. М.: Юрлитинформ, 2019. 383 с.

15. Фролова Е. Ю. Методика расследования коррупционной деятельности в правоохранительных и судебных органах: дис. … канд. юрид. наук. Краснодар, 2005. 217 с.

REFERENCES

1. Meshcheryakov V. A. Crimes in the field of computer information: legal and criminalistic analysis. Voronezh: Voronezh State University, 2001. 255 p. (In Russ.)

2. Agibalov V. Yu. The criminalistic essence of virtual traces // Bulletin of Voronezh State University. Series: Law. 2009. No. 2. P. 350–355. (In Russ.)

3. Smushkin A. B. Virtual traces in criminalistics // Legality. 2012. Issue 8. P. 43-45. (In Russ.)

4. Vekhov V. B. Fundamentals of criminalistic teaching on the study and use of computer information and its processing tools. Volgograd: Volgograd academy of the Ministry of Internal Affairs of Russia, 2008. 404 p. (In Russ.)

5. Vekhov V. B. Electronic traces in the system of criminalistics // Forensic examination. 2016. No. 2. P. 10–18. (In Russ.)

6. Bagmet A. M. Digital traces of crimes: monograph. M.: Prospect, 2021. 168 p. (In Russ.)

7. Rossinskaya E. R. The concept of digital traces in criminalistics // Aubakirov readings: proceedings of the international scientific and practical conference. Almaty, 2019. P. 6–9. (In Russ.)

8. Volevodz A. G. Countering computer crimes: legal foundations of international cooperation. Moscow: Yurlitinform, 2002. 496 p. (In Russ.)

9. Meshcheryakov V. A. Virtual traces under the "Occam scalpel" // Information security of regions. 2009. No. 1. P. 28–33. (In Russ.)

10. Rossinskaya E. R. Theory of information and computer support for forensic activities. Moscow: Prospekt, 2022. 256 p. (In Russ.)

11. Rossinskaya E. R. Problems of using special knowledge in the judicial study of computer crimes in the context of digitalization // Bulletin of the University named after O. E. Kutafin (MSAL). 2019. No. 5. P. 35–36. (In Russ.)

12. Boyarkina L. A. Digital footprint and digital shadow as derivatives of personal data // Collections of conferences of SIC "Sociosphere". 2016. No. 62. P. 78–81. (In Russ.)

13. Semikalenova A. I. The use of special knowledge in the detection and fixation of digital traces: an analysis of modern practice // Current problems of Russian law. 2019. No. 6 (103). P. 178–184. (In Russ.)

14. Zuev S. V. Fundamentals of the theory of electronic evidence: monograph. Moscow: Yurlitinform, 2019. 383 p. (In Russ.)

15. Frolova E. Y. Methodology of investigation of corruption activities in law enforcement and judicial bodies: dis. ... Cand. of Law. Krasnodar, 2005. 217 p. (In Russ.)

***Информация об авторе*:**

Е. В. Христинина, кандидат юридических наук, доцент.

Information about the author:

E. V. Khristinina, Candidate of Law, Associate Professor.

Статья поступила в редакцию 06.12.2024; одобрена после рецензирования 27.01.2025; принята к публикации 20.06.2025.

The article was submitted 06.12.2024; approved after reviewing 27.01.2025; accepted for publication 20.06.2025.