Расследование преступлений: проблемы и пути их решения. 2026. № 3. С. 148—156.
Investigation of Crimes: problems and solution, 2026, no. 3, pp. 148–156.

УДК 343.985
doi: 10.54217/2411-1627.2026.53.3.017

NIION: 2015-0064-03/26-408
MOSURED: 77/27-009-2026-03-607

Научная специальность: 5.1.4. Уголовно-правовые науки

Отдельные особенности установления криминалистически значимой информации в условиях цифровизации

Виталий Билалуевич Хазизулин[1, 2]
[1]Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации, Владивосток, Россия, hazizulinvitali@mail.ru
[2]Владивостокский государственный университет, Владивосток, Россия

Аннотация. В статье рассматриваются отдельные особенности установления криминалистически значимой информации посредством выявления и сбора цифровых следов на соответствующих носителях и в киберпространстве. Раскрывается суть таких следов со ссылкой на их классификацию. Приводятся практические примеры использования этих следов в доказывании, и определяется их значимость. Демонстрируются некоторые возможности цифровой среды для установления обстоятельств, подлежащих доказыванию. Определяется криминалистически значимая информация, выявляемая посредством использования возможностей информационно-телекоммуникационных технологий.

Ключевые слова: цифровой след; цифровая информация; цифровая среда; следователь; информационно-телекоммуникационные технологии; криминалистически значимая информация; интернет-сайт; доказательство; доказывание.

Для цитирования: Хазизулин В.Б. Отдельные особенности установления криминалистически значимой информации в условиях цифровизации // Расследование преступлений: проблемы и пути их решения. 2026. № 3. С. 148—156. doi: 10.54217/2411-1627.2026.53.3.017.

Individual features of establishing criminally relevant information in a digitalized environment

Vitaly B. Khazizulin[1, 2]
[1]Far Eastern Law Institute (Branch) of the University of the Prosecutor's Office of the Russian Federation, Vladivostok, Russia, hazizulinvitali@mail.ru
[2]Vladivostok State University, Vladivostok, Russia

Abstract. The article examines the individual features of establishing criminally relevant information by identifying and collecting digital traces on the appropriate carriers and in cyberspace. The essence of such traces is revealed with reference to their classification. The article provides practical examples of the use of these traces in evidence and identifies their significance. Some digital environment capabilities are demonstrated to establish circumstances that need to be proven. The author defines the information that is of significant forensic value and that is detected using the capabilities of information and telecommunications technologies.

Keywords: digital trail; digital information; digital environment; investigator; information and telecommunication technologies; criminally relevant information; website; evidence; proof.

For citation: Khazizulin, V.B. (2026) Individual features of establishing criminally relevant information in a digitalized environment. *Investigation of Crimes: problems and solution*, no. 3, pp. 148—156. (In Russ.). doi: 10.54217/2411-1627.2026.53.3.017.

© Хазизулин В.Б., 2026

Стремительное развитие информационно-коммуникационных технологий (ИКТ), несомненно, влияет на качество человеческой жизни, так как современные средства массовой коммуникации и распространения информации имеют всеобъемлющий характер, создавая новые социальные реалии. В то же время, как подчёркивает Председатель СК России А.И. Бастрыкин, такое развитие ИКТ «неизбежно влечёт за собой рост преступности с их применением»[1].

С таким утверждением, безусловно, следует согласиться, учитывая сохраняющуюся тенденцию к росту числа уголовно наказуемых деяний в рассматриваемой сфере[2].

При этом, как отмечено в Генеральной прокуратуре РФ, повсеместное развитие и совершенствование компьютерных технологий, расширение производства технических устройств и сферы их применения, широкая доступность компьютерной техники кроме упрощения различных технологических и бытовых процессов способствуют появлению новых видов преступных посягательств, объектами которых являются информация, информационно-телекоммуникационные ресурсы, а также денежные средства, находящиеся в обращении глобальных и локальных компьютерных сетей[3].

Однако необходимо заметить, что любое использование ИКТ сопряжено с оставлением цифровых следов в определённой автоматизированной информационной системе как в комплексе средств, позволяющих обеспечить непрерывное протекание информационных процессов[4], или в электронной (цифровой) среде[5]. Под такими следами, как пишет А.А. Бессонов, понимается «информация, зафиксированная в цифровом формате, содержащаяся в электронно-вычислительных машинах и иных цифровых устройствах, созданных на основе их технологий, в средствах подвижной радиотелефонной связи и на различных носителях цифровой информации, причинно связанная с событием преступления, позволяющая установить обстоятельства совершенного преступления и преступника»[6].

К цифровым устройствам относятся компьютерные устройства (персональные компьютеры, ноутбуки, планшеты, смартфоны) либо любые внешние электронные носители (диски, в том числе жесткие диски-накопители, флеш-карты и т. п.)[7], а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека[8].

Отметим, что цифровая информация может также содержаться в распространенных в настоящее время облачных хранилищах, где «данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам»[9].

Учитывая характер содержащейся на таких устройствах и в хранилищах информации, можно сделать вывод, что она способна раскрывать сведения о лице, причастном к её созданию. К этим сведениям относятся данные о возрасте, половой принадлежности, гражданстве, привычках, геолокации и пр.

---

[1] Интервью Председателя СК России изданию «IT-World». 30.10.2025 // СК России: офиц. сайт. URL: https://sledcom.ru/press/interview/item/2032072 (дата обращения: 26.02.2026).

[2] Число IT-преступлений в 2024 году достигло рекордных значений // Эксперт. 27.01.2025. URL: https://expert.ru/news/chislo-it-prestupleniy-v-2024-godu-dostiglo-v-rossii-rekordnykh-765-4-tys (дата обращения: 26.02.2026).

[3] Письмо Генпрокуратуры России от 13.09.2023 № 36-49-2023 «О Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утв. Генпрокуратурой России» // СПС КонсультантПлюс.

[4] Переверзева Е.С., Комов А.В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 175.

[5] ГОСТ Р 52292—2004. Информационная технология. Электронный обмен информацией. Термины и определения: национальный стандарт Российской Федерации: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2004 г. № 135-ст // СПС КонсультантПлюс.

[6] Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. 2019. № 3. С. 47.

[7] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // СПС КонсультантПлюс.

[8] Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершённых с использованием информационно-телекоммуникационных технологий: научно-практическое пособие / [А.С. Анненкова, А.Л. Аристархов, К.В. Васильченко и др.]. М., 2023. С. 10.

[9] Рамалданов Х.Х. Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. 2022. № 1 (60). С. 127.

Кроме того, работая и общаясь в цифровой среде, сохраняя в ней информацию либо исследуя её, человек оставляет в ней средства своей индивидуализации, которыми могут быть адрес электронной почты, аватар и т. п. При этом, как отмечает Э.В. Талапина, «в виртуальном пространстве субъект часто прячется за так называемой виртуальной личностью, или цифровым образом»[10]. Это утверждение абсолютно верно демонстрирует фактические обстоятельства, зачастую встречающиеся в следственно-судебной практике, когда преступное поведение предполагает общение потенциального потерпевшего с образами, симуляциями, а не с реальным субъектом[11].

> Так, Д. с помощью принадлежащего ему мобильного телефона с определённым IP-адресом создал в одной из социальных сетей несколько интернет-страниц вымышленных лиц, посредством которых вступал в диалог со своими жертвами, совершая в отношении них преступления против половой неприкосновенности[12].

И подобные примеры не единичны, в то время как цифровые образы граждан широко используются в соответствующем пространстве[13].

Исследователи отмечают, что цифровые следы в зависимости от формы их выражения классифицируются на активные и пассивные[14]. При этом первые из них создаются данными, предоставляемыми пользователем ИКТ (фотографии и комментарии, размещаемые в социальных сетях, персональные данные, доменные имена, удалённые файлы и т. п.). Вторые — это данные, которые ненамеренно оставляют лица, использующие ИКТ (cookie-файлы, log-файлы, геолокация и т. п.).

С учётом такой классификации к пассивным цифровым следам также можно относить и соответствующие сведения о качестве и безопасности товаров, их составе, данные о движении от производителя до продавца и т. п. Их выявление и фиксация с криминалистической точки зрения могут эффективно осуществляться, например, посредством Государственной информационной системы мониторинга за оборотом товаров (ГИС МТ).

Изучение материалов правоприменения (уголовных дел, контрольных и надзорных производств, приговоров судов и т. п.) и научной литературы свидетельствует о достаточно распространённой практике использования цифровых следов в уголовном судопроизводстве. Особенно актуально их применение в криминалистическом профилировании личности неизвестного преступника[15], который оставил определённые следы в цифровой среде.

Именно поэтому рассматриваемое направление криминалистической деятельности получило название «цифровая криминалистика»[16], что имеет непосредственное отношение к процессу сбора, получения, сохранения, анализа и исследования электронных (цифровых) доказательств.

Соответствующая поисково-познавательная деятельность следователя детерминирована закономерностями механизмов преступления, способа его сокрытия, а также следообразования, которые тем или иным способом связаны с информацией, зафиксированной в цифровом формате. Эти механизмы обусловливают возникновение в цифровой среде и в связанных с ней цифровых устройствах криминалистически значимой информации, в том числе о самом преступлении и о его участниках. Она возникает в результате процессов взаимодействия преступника и других связанных с преступным событием лиц с указанной средой, отражаясь в ней в виде цифровых следов.

Наличие таких следов учёными-криминалистами выделяется как специфический признак преступлений, совершённых с использованием ИКТ. При этом они признаются «основным источником криминалистически значимой информации, обнаружение, фиксация, изъятие и иссле-

---

[10] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 6.

[11] Пучков Д.В. Обыденное и альтернативное цифровое сознание: проблема уголовно-правового сопряжения // Евразийский юридический журнал. 2020. № 6 (145). С. 291.

[12] Контрольное производство по уголовному делу № 12102050022000063 // Архив СУ СК России по Приморскому краю. 2022.

[13] См., напр.: Новокшонова Н.А. Цифровая идентификация гражданина: современные вызовы // Вестник Челябинского государственного университета. Серия: Право. 2025. Т. 10, № 2. С. 5—12.

[14] 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. 142.

[15] Бахтеев Д.В., Леднёв И.В. Понятие и свойства криминалистического профилирования личности и поведения неизвестного преступника // Юридическая наука и правоохранительная практика. 2020. № 3 (53). С. 110—118.

[16] См., напр.: Цифровая криминалистика: учебник для вузов / под ред. В.Б. Вехова, С.В. Зуева. 3-е изд., перераб. и доп. М., 2026; Дяблова Ю.Л. Цифровая криминалистика — будущее науки или тренд современности? // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 1. С. 85—93.

дование которых невозможно без использования информационных технологий»[17].

Массовое использование в уголовном судопроизводстве цифровых следов обусловило необходимость корректировки действующего законодательства, которая направлена на регламентацию порядка работы с такими доказательствами. Так, например, законодатель определил порядок изъятия в ходе следственных действий электронных носителей информации[18] и цифровой валюты[19], участие в обороте которой оставляет цифровые следы.

В то же время традиционные подходы к расследованию преступлений также столкнулись с необходимостью корректировки для их адаптации к новым реалиям, где цифровые данные могут использоваться для подтверждения или опровержения какого-либо факта, показаний участников уголовного судопроизводства, причастности (непричастности) лица к совершению преступления.

Так, по уголовному делу по обвинению бывшего заместителя главы администрации г. Владивостока Л. в получении взятки спустя более шести лет после преступного события удалось установить, что абонентские номера взяткодателя и чиновника во время совершения преступления в 2018 году совместно фиксировались базовой станцией, расположенной в районе рабочего места последнего. Также в ходе осмотра мобильного телефона взяткодателя установлено, что в приложении «Контакты» имелся абонентский номер Л. и соответствующая ссылка на его владельца, а в приложении мессенджера имелась совместная группа указанных лиц с перепиской между ними. При этом созданы они были до даты совершения преступления.

Перечисленные цифровые следы, процессуально закреплённые в протоколе осмотра предметов (документов), оценены судом в качестве доказательств, объективно подтверждающих достоверность показаний взяткодателя о времени, месте и обстоятельствах передачи им взятки[20].

Другим наглядным примером использования мобильных телефонов в процессе доказывания является выявление пассивных следов в виде истории браузера, которая автоматически генерируется в процессе эксплуатации поисковых систем для просмотра той или иной информации в информационно-телекоммуникационных сетях.

Таким образом установлены факты неоднократного посещения гражданином К. интернет-сайтов, содержащих специфическую информацию, позволяющую установить наличие у него интереса к иным действиям сексуального характера в отношении несовершеннолетних. Эти данные положены в обоснование мотива и цели при исследовании соответствующего преступного поведения и квалификации его деяния[21].

Рассматривая подобные примеры, следует заметить, что ещё профессор Г.А. Густов выделял, в частности, такие специфические закономерности расследования, как зависимость действий следователя от обстановки, в которой проводится расследование, и предопределённость выбора методов, средств, приёмов расследования профессионализмом и другими психофизическими качествами следователя, его активностью и волей[22].

Разделяя такое утверждение, важно подчеркнуть, что наличие цифровой криминалистически значимой информации определяет действия следователя (следователя-криминалиста) по выявлению и сбору доказательств в киберпространстве. При этом с учётом скорости оборота цифровой информации осуществлять соответствующие действия при определённых обстоятельствах возможно в максимально короткие сроки.

Так, в ходе осмотра места происшествия по факту убийства Ч. в его квартире обнаружена бутылка из-под спиртного напитка с содержащейся на

[17] Антонов О.Ю. Общие положения методики расследования преступлений, совершённых с использованием информационных технологий // Расследование преступлений: проблемы и пути их решения. 2026. № 1. С. 45.

[18] Федеральный закон от 27.12.2018 № 533-ФЗ «О внесении изменений в статьи 76.1 и 145.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // СПС КонсультантПлюс.

[19] Федеральный закон от 20.02.2026 № 38-ФЗ «О внесении изменений в статью 104.1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202602200059 (дата обращения: 26.02.2026).

[20] Уголовное дело № 1-135/2024 // Архив Первореченского районного суда г. Владивостока. 2024.

[21] Контрольное производство по уголовному делу № 12202050018000006 // Архив СУ СК России по Приморскому краю. 2022.

[22] Густов Г.А. Проблемы методов научного познания в организации расследования преступлений: дис. ... д-ра юрид. наук в форме научного доклада. М., 1993. С. 8.

ней акцизной маркой. Путём её сканирования с использованием специализированного мобильного приложения Росалкогольтабакконтроля следователем-криминалистом уже в процессе осмотра места происшествия получена информация о времени и месте розничной продажи этой бутылки. В результате следственно-оперативная группа незамедлительно прибыла в магазин продажи алкогольной продукции, в котором были обнаружены и изъяты видеозаписи камер внутреннего и наружного наблюдения. Их осмотром установлено, что в определённое время Ч. совместно с Г. приобрели в этом магазине бутылку спиртного напитка, после чего ушли из него. Эти видеозаписи позволили идентифицировать Г. и оперативно произвести следственные действия, направленные на изобличение его причастности к убийству Ч.[23]

Приведённый пример демонстрирует зависимость действий субъекта расследования от окружающей обстановки, в которой обнаружен материальный след. При этом информация о его обороте, содержащаяся в цифровой среде, предопределила выбор метода и средства установления лица, причастного к совершению преступления.

В практике встречаются случаи, когда обнаруженный цифровой след выступает основополагающим доказательством, дополняя всю совокупность имеющихся косвенных доказательств.

Например, в ходе исследования мобильного телефона потерпевшей в рамках компьютерно-технической судебной экспертизы посредством восстановления ранее содержавшейся в гаджете информации обнаружена изготовленная электронным способом предсмертная записка, в которой потерпевшая подробно излагала обстоятельства совершённых против неё преступных действий, связанных с доведением её до самоубийства. В результате именно эта процессуально закреплённая цифровая информация явилась фундаментом среди собранных по уголовному делу доказательств, что позволило суду вынести обвинительный приговор.
Стоит также отметить, что полученные посредством информационно-аналитического исследования следователем-криминалистом сведения о потерпевшей в открытых источниках сети Интернет, в том числе о её связях в социальных сетях, также выступили доказательственной информацией по данному делу[24].

Из приведённого примера видно, что иногда именно мобильный телефон может выступать лучшим «свидетелем» совершённого преступления. К таким же доказательствам могут относиться умные очки или смарт-часы, посредством которых возможно установить сведения о навигации их пользователя или о бесконтактной оплате товаров и пр.

Общеизвестно, что используемые нами смартфоны и другие электронные устройства с момента внедрения в нашу жизнь хранят в себе значительный объем цифровой информации. Переписка, фотографии, географические данные, телефонная книга, копии документов и т. п. — все эти сведения могут содержать криминалистически значимую информацию и иметь существенное значение для уголовного судопроизводства. Даже голосовое сообщение в мессенджере может использоваться в качестве образца для сравнительного исследования при производстве фоноскопической судебной экспертизы в случае, если обвиняемый отказывается давать следователю образец своего голоса[25].

При этом современные программные комплексы позволяют извлекать указанную информацию из различных устройств, облачных сервисов и даже беспилотных летательных аппаратов вне зависимости от того, хранится ли она в их памяти или была удалена.

Очевидно, что сейчас следователь не может не обращать своё внимание на цифровые следы преступления и не использовать их в установлении обстоятельств, подлежащих доказыванию. При этом он имеет возможность применять собственные знания в сфере ИКТ в пределах процессуальных полномочий, например, для осмотра интернет-сайта. Кроме того, следователь «вправе привлечь к участию в следственном действии специалиста» (ст. 168 УПК РФ)[26] и использовать его специальные знания, в частности в области компьютерных систем, сетей и программного обеспечения, в процессе сбора доказательств.

Следует обратить внимание, что эффективность применения тех и других знаний требует творческого подхода для того, чтобы через технику их использования достигать не только ближайших (сбор, получение, сохранение информации в цифровой среде), но и отдалённых целей,

[23] Уголовное дело № 1-8/2023 // Архив Булунского районного суда Республики Саха (Якутия). 2023.
[24] Уголовное дело № 1-15/2024 // Архив Уссурийского районного суда Приморского края. 2022.
[25] Уголовное дело № 1-17/2025 // Архив Надеждинского районного суда Приморского края. 2025.
[26] Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ // СПС КонсультантПлюс.

заключающихся в познании общих закономерностей формирования цифровых следов и понимании их значения для расследования преступления.

Таким образом, особенности правоприменения в настоящее время обусловливают целесообразность широкого использования цифровых следов в процессуальном познании и доказывании. Соответствие же криминалистической деятельности закономерностям научно-технического прогресса выступает одним из свидетельств её эффективности.

Однако такая деятельность должна фокусироваться не только на выявлении непосредственно цифровых следов с точки зрения восприятия их в качестве источника информации ушедшего в прошлое события. В условиях цифровизации особое внимание также заслуживают и другие возможности «информационно-компьютерного обеспечения криминалистической деятельности»[27]. Оно также позволяет следователю получать новую доказательственную или ориентирующую информацию либо проверять уже имеющиеся сведения, используя общие закономерности выявления, фиксации, сохранения и исследования информации о преступлении и о его участниках.

Например, Система межведомственного электронного взаимодействия предоставляет актуальные данные ФНС России и Росреестра о доходах и имуществе физического или юридического лица, о наличии у них банковских счетов, об их реквизитах и т. п.

Возможности официального сайта ФНС России позволяют получить выписку из ЕГРЮЛ/ЕГРИП в отношении юридического лица или индивидуального предпринимателя, которая надлежаще заверена и подписана электронной подписью уполномоченного должностного лица. Она, в частности, предоставляет сведения о руководителе и адресе юридического лица, о его учредителях, об их долях в уставном капитале организации и о его сумме, об основных видах деятельности компании и пр. В отношении акционерных обществ такая выписка необходима для получения сведений о держателе реестра акционеров, что в дальнейшем позволяет истребовать у него этот реестр и установить информацию о зарегистрированных в нём лицах и проведённых операциях по принадлежащим им акциям.

Интернет-сайты организаций также могут содержать доказательственную либо ориентирующую информацию.

> Так, например, в процессе осмотра интернет-сайтов региональной адвокатской палаты и одного из адвокатских образований в протоколе осмотра предметов (документов, электронного ресурса) отражены сведения о конкретных адвокатах (анкетные данные, образование, трудовой и профессиональный стаж, специализация, адреса и номера телефонов, электронная почта, регистрационный номер в реестре адвокатов и пр.), в отношении которых возбуждено уголовное дело. В последующем эти данные использованы в процессе доказывания, в том числе при получении разрешения суда на производство осмотра служебных помещений, используемых для осуществления адвокатской деятельности[28].
>
> Аналогично осмотрен официальный сайт районного суда с фиксацией сведений о периоде рассмотрения уголовного дела, в котором ранее участвовали указанные защитники при совершении преступных действий, а также автомобильный интернет-портал для установления сведений о рыночной стоимости автомобиля подозреваемого в целях наложения на него ареста[29].

В следственно-судебной практике встречаются факты установления криминалистически значимой информации об отдельных специфических товарах, используемых при совершении определённых преступлений, с интернет-сайтов. При этом такая информация может находить своё отражение в фабуле предъявленного субъекту преступления обвинения[30].

В процессе расследования обстоятельств закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд указанную информацию возможно оперативно получить посредством осмотра официального сайта Единой информационной системы в сфере закупок, где содержится информация о субъектах закупок, о соответствующих контрактах, документах, связанных с их заключением и исполнением[31].

---

[27] Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193—202.

[28] Уголовное дело № 1-162/2023 // Архив Центрального районного суда г. Хабаровска. 2023.

[29] Там же.

[30] Контрольное производство по уголовному делу № 12102050032000020 // Архив СУ СК России по Приморскому краю. 2022.

[31] Реестр контрактов, заключенных заказчиками. URL: https://zakupki.gov.ru/epz/contract/search/results.html (дата обращения: 30.10.2025).

В организациях, являющихся владельцами социальных сетей, мессенджеров, иных интернет-ресурсов и сервисов, возможно истребовать данные о датах и времени их посещения, IP-адресах устройств, использовавшихся для входа в сеть, об абонентах, которым предоставлена в пользование емкость соответствующих IP-адресов, и адресах их проживания (либо юридических адресах), а также содержание личной переписки (на основании постановления суда).

Сведения о заказе товара посредством широко используемых мобильных приложений и о его получении в определённом месте также могут использоваться в процессе доказывания, определяя местонахождение покупателя и момент соответствующего действия.

В публичных справочных правовых системах содержатся актуальные сведения о курсе валют Банка России на конкретную дату определённого года за несколько десятков последних лет. Его установление необходимо, в частности, по уголовным делам коррупционной направленности, где предметом преступления выступает иностранная валюта.

Перечисленные способы получения криминалистически значимой информации из сети Интернет, облачных хранилищ и цифровых устройств не являются исчерпывающими, а лишь отражают некоторые возможности для её обнаружения, фиксации, изъятия и исследования. При этом такая информация может прямо не указывать на субъекта преступления, а использоваться для установления определённых обстоятельств (сведений), имеющих отношение к расследуемому преступлению.

В результате данные, получаемые с использованием ИКТ, могут выступать как прямыми доказательствами, устанавливающими какой-либо факт, так и косвенными доказательствами, обосновывающими вывод об истинности того или иного события. Тем самым они являются цифровыми доказательствами, представляющими собой электронную информацию, имеющую значение для установления обстоятельств, подлежащих доказыванию[32], с использованием принципа расследования «от цифровой информации (следа) к преступнику».

В завершение можно констатировать, что в современных условиях знание особенностей, свойственных новейшим ИКТ, и понимание возможностей получения с их использованием криминалистически значимой информации является безусловным залогом качественного сбора доказательств по уголовному делу. При этом порой без использования электронной информации вовсе невозможно сформировать обоснованное суждение об имеющих уголовно-правовое значение обстоятельствах, что предполагает развитие соответствующих знаний, умений и навыков у субъекта расследования и их практическое применение.

[32] Рамалданов Х.Х. Указ. соч. С. 127.

Список литературы

1. Антонов О.Ю. Общие положения методики расследования преступлений, совершённых с использованием информационных технологий // Расследование преступлений: проблемы и пути их решения. 2026. № 1. С. 43—53. doi: 10.54217/2411-1627.2026.51.1.006.

2. Бахтеев Д.В., Леднёв И.В. Понятие и свойства криминалистического профилирования личности и поведения неизвестного преступника // Юридическая наука и правоохранительная практика. 2020. № 3 (53). С. 110—118.

3. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. 2019. № 3. С. 46—52. doi: 10.17803/2311-5998.2019.55.3.046-052.

4. 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.

5. Густов Г.А. Проблемы методов научного познания в организации расследования преступлений: дис. ... д-ра юрид. наук в форме научного доклада. М., 1993. 59 с.

6. Дяблова Ю.Л. Цифровая криминалистика — будущее науки или тренд современности? // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 1. С. 85—93. doi: 10.24412/2071-6184-2021-1-85-93.

7. Новокшонова Н.А. Цифровая идентификация гражданина: современные вызовы // Вестник Челябинского государственного университета. Серия: Право. 2025. Т. 10, № 2. С. 5—12. doi: 10.47475/2618-8236-2025-10-2-5-12.

8. Переверзева Е.С., Комов А.В. Виртуальные и цифровые следы: новый подход в понимании // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 172—178. doi: 10.35750/2071-8284-2021-1-172-178.

9. Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершённых с использованием информационно-телекоммуникационных технологий: научно-практическое пособие / [А.С. Анненкова, А.Л. Аристархов, К.В. Васильченко и др.]. М.: Университет прокуратуры Российской Федерации, 2023. 122 с.

10. Пучков Д.В. Обыденное и альтернативное цифровое сознание: проблема уголовно-правового сопряжения // Евразийский юридический журнал. 2020. № 6 (145). С. 290—293. doi: 10.46320/2073-4506-2020-6-145-290-293.

11. Рамалданов Х.Х. Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. 2022. № 1 (60). С. 121—128. doi: 10.25724/VAMVD.ZDEF.

12. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193—202. doi: 10.24411/2312-3184-2019-00019.

13. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5—17. doi: 10.12737/art_2018_2_1.

14. Цифровая криминалистика: учебник для вузов / под ред. В.Б. Вехова, С.В. Зуева. 3-е изд., перераб. и доп. М.: Юрайт, 2026. 485 с.

References

1. Antonov, O.Yu. (2026) Obshchie polozheniya metodiki rassledovaniya prestupleniy, sovershennykh s ispol'zovaniem informatsionnykh tekhnologiy [General provisions of the methodology for investigating crimes with the use of information technology]. *Investigation of Crimes: problems and solution*, no. 1, pp. 43–53. (In Russ.). doi: 10.54217/2411-1627.2026.51.1.006.

2. Bakhteev, D.V., Lednev, I.V. (2020) Ponyatie i svoystva kriminalisticheskogo profilirovaniya lichnosti i povedeniya neizvestnogo prestupnika [The concept and characteristics of forensic profiling of the personality and behavior of an unknown offender]. *Legal Science and Law Enforcement Practice*, no. 3, pp. 110–118. (In Russ.).

3. Bessonov, A.A. (2019) O nekotorykh vozmozhnostyakh sovremennoy kriminalistiki v rabote s elektronnymi sledami [On some possibilities of modern forensic science in working with electronic traces]. *Vestnik Universiteta imeni O.E. Kutafina*, no. 3, pp. 46–52. (In Russ.). doi: 10.17803/2311-5998.2019.55.3.046-052.

4. Buynov, D.O. (2022) Vidy tsifrovykh 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 rossiyskogo prava*, vol. 17, no. 11, pp. 140–148. (In Russ.). doi: 10.17803/1994-1471.2022.144.11.140-148.

5. Gustov, G.A. (1993) Problemy metodov nauchnogo poznaniya v organizatsii rassledovaniya prestupleniy [Problems related to the methods of scientific cognition in organizing crime investigation]. Doctor's degree dissertation. Moscow, 59 p. (In Russ.).

6. Dyablova, Yu.L. (2021) Tsifrovaya kriminalistika – budushchee nauki ili trend sovremennosti? [Digital forensics – the future of science or the trend of our time?] *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki*, no. 1, pp. 85–93. (In Russ.). doi: 10.24412/2071-6184-2021-1-85-93.

7. Novokshonova, N.A. (2025) Tsifrovaya identifikatsiya grazhdanina: sovremennye vyzovy [Digital identification of citizens: modern challenges]. *Bulletin of Chelyabinsk State University. Series: Law*, vol. 10, no. 2, pp. 5–12. (In Russ.). doi: 10.47475/2618-8236-2025-10-2-5-12.

8. Pereverzeva, E.S., Komov, A.V. (2021) Virtual'nye i tsifrovye sledy: novyy podkhod v ponimanii [Virtual and digital traces: a new approach in understanding]. *Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia*, no. 1, pp. 172–178. (In Russ.). doi: 10.35750/2071-8284-2021-1-172-178.

9. University of the Prosecutor's Office of the Russian Federation. (2023) *Prokurorskiy nadzor za ispolneniem zakonov organami predvaritel'nogo rassledovaniya pri vyyavlenii i rassledovanii prestupleniy, sovershennykh s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologiy [Prosecutorial supervision over the observance of laws by the bodies conducting preliminary investigations in the detection and investigation of crimes committed using information and telecommunications technologies.]*. Moscow, 122 p. (In Russ.).

10. Puchkov, D.V. (2020) Obydennoe i al'ternativnoe soznanie: problema ugolovno-pravovogo sopryazheniya [Ordinary and alternative digital consciousness: the problem of criminal-legal interface]. *Eurasian Law Journal*, no. 6, pp. 290–293.

(In Russ.). doi: 10.46320/2073-4506-2020-6-145-290-293.

11. Ramaldanov, Kh.Kh. (2022) Ponyatie i sushchnost' tsifrovizatsii dokazatel'stv i dokazyvaniya v ugolovnom sudoproizvodstve [The concept and essence of digitalization of evidence and proof in criminal proceedings]. *Vestnik Volgogradskoy akademii MVD Rossii*, no. 1, pp. 121–128. (In Russ.). doi: 10.25724/VAMVD.ZDEF.

12. Rossinskaya, E.R. (2019) Teoriya informatsionno-komp'yuternogo obespecheniya kriminalisticheskoy deyatel'nosti: kontseptsiya, sistema, osnovnye zakonomernosti [Theory of information and computer support of criminalistic activity: concept, system, basic patterns]. *Vestnik Vostochno-Sibirskogo instituta MVD Rossii*, no. 2, pp. 193–202. (In Russ.). doi: 10.24411/2312-3184-2019-00019.

13. Talapina, E.V. (2018) Pravo i tsifrovizatsiya: novye vyzovy i perspektivy [Law and digitalization: new challenges and prospects]. *Journal of Russian Law*, no. 2, pp. 5–17. (In Russ.). doi: 10.12737/art_2018_2_1.

14. Vekhov, V.B., Zuev, S.V. (eds.) (2026) Tsifrovaya kriminalistika [Digital forensics]. Textbook. Moscow, Urait, 485 p. (In Russ.).

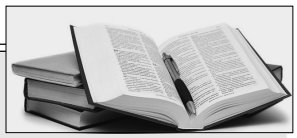
Информация об авторе

В.Б. Хазизулин — заведующий кафедрой уголовно-правовых дисциплин Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, доцент кафедры уголовно-правовых дисциплин Института права Владивостокского государственного университета, кандидат юридических наук.

Information about the author

V.B. Khazizulin – Head of the Department of Criminal Law Disciplines of the Far Eastern Law Institute (Branch) of the University of the Prosecutor's Office of the Russian Federation, Associate Professor of the Department of Criminal Law Disciplines of the Institute of Law of the Vladivostok State University, Candidate of Law.

ИЗДАТЕЛЬСТВО «ЮНИТИ-ДАНА» ПРЕДСТАВЛЯЕТ





Административная ответственность. 10-е изд., перераб. и доп. Учебное пособие. Гриф УМЦ "Профессиональный учебник". Гриф НИИ образования и науки. —351 с. / Под ред. О.В. Зиборова, А.И. Стахова.

ISBN: 978-5-238-03851-3

Рассматриваются ключевые вопросы административной ответственности как института административного права. Анализируются материально-правовые и процессуальные основания административной ответственности, система и виды административных наказаний, общие и особые правила их назначения, структура и механизм производства по делам об административных правонарушениях. Исследуется специфика административно-деликтного производства в арбитражных судах.

Для студентов, аспирантов, преподавателей юридических вузов, сотрудников органов, обладающих административно-юрисдикционнными полномочиями, а также всех интересующихся проблемами административной ответственности.