DOI: 10.17803/1994-1471.2025.170.1.188-196

К. Т. Саркисян*

Проблемы собирания цифровых следов при производстве следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях

Аннотация. В статье рассматриваются актуальные вопросы обнаружения, фиксации и изъятия цифровых следов в рамках следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях. Анализируются основные подходы к пониманию цифрового следа, а также позиции по классификации цифровых следов. Указывается, какие конкретно цифровые следы встречаются в такой категории дел, как незаконный оборот наркотических средств в компьютерных сетях. Автором проведен анализ международного опыта в области собирания цифровых следов, изучена отечественная судебная практика по рассматриваемой категории дел. Приводятся примеры, иллюстрирующие актуальность данной темы. В ходе проведения исследования выявлены проблемы, возникающие при собирании цифровых следов в рамках производства таких следственных действий, как осмотр и обыск. Отмечается необходимость разработки методики, направленной на стандартизацию порядка работы с цифровыми следами.

Ключевые слова: цифровые следы; собирание цифровых следов; классификация цифровых следов; наркотические средства; наркопреступность; незаконный оборот наркотических средств; компьютерные сети; Даркнет; маскировка; специальные знания.

Для цитирования: *Саркисян К. Т.* Проблемы собирания цифровых следов при производстве следственных действий по делам, связанным с незаконным оборотом наркотических средств в компьютерных сетях // Актуальные проблемы российского права. — 2025. — Т. 20. — № 1. — С. 188–196. — DOI: 10.17803/1994-1471.2025.170.1.188-196.

Problems of Collecting Digital Traces during Investigative Activities in Cases Related to Illegal Drug Trafficking in Computer Networks

Karina T. Sarkisyan, Postgraduate Student, Department of Forensic Expertise, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
karina8888883@gmail.com

Abstract. The paper examines current issues of detection, recording and seizure of digital traces in line with investigative activities in cases related to the illegal trafficking of drugs in computer networks. The main approaches to understanding a digital trace, as well as positions on the classification of digital traces, are considered. The paper analyzes what specific digital traces are encountered in such a category of cases as illegal drug trafficking in

* *Саркисян Карина Тархановна*, аспирант кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Российская Федерация, 125993
karina8888883@gmail.com

computer networks. An analysis of international experience in the field of collecting digital traces was conducted, and domestic judicial practice in the category of cases under consideration was studied. Examples are given to illustrate the relevance of this topic. During the study, problems were identified that arise when collecting digital traces during investigative actions such as inspection and search. The paper notes the need to develop a methodology aimed at standardizing the procedure for working with digital traces.
Keywords: digital traces; digital trace collection; digital trace classification; narcotics; drug crime; drug trafficking; computer networks; Darknet; disguise; special knowledge.
Cite as: Sarkisyan KT. Problems of Collecting Digital Traces during Investigative Activities in Cases Related to Illegal Drug Trafficking in Computer Networks. *Aktual'nye problemy rossijskogo prava*. 2025;20(1):188-196. (In Russ.). DOI: 10.17803/1994-1471.2025.170.1.188-196.

Современные технологии и повсеместная цифровизация оказали свое влияние на развитие и изменение юридических наук, в частности уголовно-правовых. Как показывает практика, процессы цифровизации привели к появлению нового вида следов, а именно цифровых следов. Вопросы, связанные с понятием «цифровой след», активно обсуждаются в научной среде и становятся объектом дискуссий ученых.

При этом важно отметить, что такая тенденция отмечается не только в России, но и в целом по всему миру.

Согласно статистике, представленной Советом начальников национальной полиции Великобритании, при расследовании более 90 % всех зарегистрированных преступлений обнаруживаются цифровые следы, которые в результате многоэтапных процессов обнаружения, фиксации и изъятия преобразуются в такой вид доказательств, как цифровые доказательства[1].

Действительно, в настоящее время большое количество преступлений совершается с использованием компьютерных средств и систем, в результате чего и появляются цифровые следы.

Прежде чем перейти к рассмотрению основных проблем собирания цифровых следов, следует определиться, что́ в науке обозначается этим термином.

Не все ученые используют понятие «цифровые следы», говоря о данных объектах. Так, например, В. А. Мещеряков в своих работах вводит понятие «виртуальные следы», под которыми понимает любое изменение состояния автоматизированной информационной системы, связанное с событием преступления, представленное в виде компьютерной информации и зафиксированное на материальном носителе[2].

В. Б. Вехов употребляет термин «электронный след», подразумевая информацию, содержащуюся на определенных электронных носителях[3].

Понятие же «цифрового следа» было разработано Е. Р. Россинской, которая предлагает понимать под цифровым следом «криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи»[4].

---

1 The National Policing Digital Strategy 2020–2030: Digital, Data and Technology Strategy (the Strategy) // URL: https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf (дата обращения: 21.01.2024).

2 *Мещеряков В. А.* Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж : Изд-во Воронежского государственного университета, 2002. С. 94–98.

3 *Вехов В. Б., Смагоринский Б. П., Ковалев С. А.* Электронные следы в системе криминалистики // Судебная экспертиза. 2016. Вып. 2. С. 14.

4 Теория информационно-компьютерного обеспечения криминалистической деятельности : монография / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский ; под ред. Е. Р. Россинской. М. : Проспект, 2022. С. 44.

Представляется, что данное определение наиболее полно, точно и емко раскрывает сущность цифрового следа.

Продолжая тему дискуссии о цифровых следах, следует сказать, что существует множество классификаций цифровых следов, к общему мнению ученые на данный момент не пришли, поэтому их позиции разнятся.

Традиционно в криминалистике следы делят на материальные и идеальные.

Р. А. Дерюгин, А. А. Жижелева считают, что цифровые следы нельзя отнести ни к материальным, ни к идеальным, поскольку они занимают промежуточное положение[5].

По мнению В. Б. Вехова, Б. П. Смагоринского, С. А. Ковалева, компьютерная информация обладает определенными фиксированными характеристиками и представляет собой «невидимые материальные следы»[6].

В связи с этим ряд авторов, в частности упомянутый В. А. Мещеряков, предлагают ввести еще одну категорию — «виртуальные следы»[7].

Однако такое деление будет не совсем корректным, так как цифровые следы всё же содержатся на материальных носителях и, что важно, неотделимы от них.

По этой причине нельзя не согласиться с мнением Е. Р. Россинской, которая пишет, что «по природе цифровые следы являются следами материальными»[8].

Развивая вопрос классификации цифровых следов, Е. Р. Россинская предлагает классификацию цифровых следов по месту хранения[9]:

1) на отдельных носителях,
2) в компьютерных системах и сетях.

В контексте преступлений, связанных с незаконным оборотом наркотических средств, наиболее актуальным является рассмотрение цифровых следов, хранящихся в компьютерных сетях.

Несмотря на то что вопросам о цифровых следах в последние годы уделяется достаточное внимание в науке, всё же отсутствие четко определенных, сформулированных правовых, теоретических и организационных основ обнаружения, фиксации и изъятия цифровых следов приводит к ситуации, когда имеющие значение для дела цифровые следы не становятся в результате процессуальных действий доказательствами. Это негативно отражается на расследовании и раскрытии преступлений правоохранительными органами.

Незаконный оборот наркотических средств во многом осуществляется с использованием информационно-телекоммуникационных сетей, в связи с чем поднимаемая проблема наиболее актуальна для наркопреступлений.

Собирание следов преступления представляет собой многоступенчатый и комплексный процесс, осуществляемый в соответствии с законодательством и существующими методиками.

Говоря о собирании следов, традиционно в криминалистике под этим понимают три последовательно сменяющих друг друга этапа: обнаружение, фиксацию и изъятие[10]. Вопросы, связанные с обнаружением, фиксацией и изъятием следов, освещаются уже достаточно давно.

При анализе работ ученых можно отметить, что для каждого объекта имеются определен-

---

[5] *Дерюгин Р. А.*, *Жижелева А. А.* Перспективы развития цифровой криминалистики в условиях информационного общества // Технологии XXI века в юриспруденции : материалы Всероссийской научно-практической конференции (Екатеринбург, 24–25 мая 2019 г.) / под ред. Д. В. Бахтеева. С. 40–46.

[6] *Вехов В. Б., Смагоринский Б. П., Ковалев С. А.* Указ. соч. С. 17.

[7] *Мещеряков В. А.* Указ. соч. С. 94–98.

[8] *Россинская Е. Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 199.

[9] Теория информационно-компьютерного обеспечения криминалистической деятельности : монография. С. 46.

[10] *Аверьянова Т. В.*, *Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов. 4-е изд., перераб. и доп. М. : Норма : Инфра-М, 2014.

ные особенности их обнаружения, фиксации и изъятия.

В случае с цифровыми следами необходимо учитывать их специфику, а также то, в рамках каких следственных действий происходит процесс собирания.

Результаты проведенного исследования демонстрируют, что в основном следователи при расследовании дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях, сталкиваются с цифровыми следами при производстве таких следственных действий, как осмотр и обыск.

В зависимости от того, какое следственное действие проходит, выстраивается тактика работы с цифровыми следами, определяется порядок проводимых с ними действий в ходе собирания.

Так, осмотр в большинстве своем требует большей оперативности по принятию решений, привлечению специалистов, нежели обыск, который проводится уже по возбужденному уголовному делу.

Возвращаясь все-таки к специфике цифровых следов, отметим, что цифровые следы представляют собой именно компьютерную информацию, то есть они сами по себе не могут быть изъяты, приобщены к материалам дела, так как информация всё же представляет собой нечто нематериальное, что нельзя воспринимать органами чувств непосредственно. Поэтому цифровые следы неотделимы от их носителей, на которых они располагаются.

Особенность цифровых следов заключается и в их доступности. Принимая во внимание уровень и степень внедрения современных технологий, сто́ит учитывать, что пользователь имеет возможность без труда и достаточно оперативно управлять компьютерной информацией, проводить с ней различные процедуры в удаленном режиме.

Данные факторы приводят к необходимости разработки новых методов и способов обнаружения, фиксации и изъятия цифровых следов.

Сложность работы с цифровыми следами состоит в том, что, помимо общих для всех цифровых следов особенностей, нужно иметь в виду также специфику отдельных видов цифровых следов.

Анализ судебной практики демонстрирует, что наиболее часто встречающимися цифровыми следами по исследуемой категории дел являются следующие:

— данные социальных сетей и мессенджеров;

— данные сайтов сети Интернет, сети Даркнет, история посещения сайтов;

— данные приложений, содержащие информацию, например о местоположении и о проведенных транзакциях;

— облачное хранилище данных.

В ходе исследования данных социальных сетей, мессенджеров, а также данных с сайтов их обнаружение может быть осложнено тем, что значимая для дела информация может быть замаскирована. Такая маскировка бывает как лингвистической, так и компьютерно-технической.

Так, в разговоре могут быть употреблены слова, фразы, которые на первый взгляд не относятся к семантическому полю «наркотические средства», однако при более детальном исследовании не только вырванных из контекста лексем, словосочетаний, но и всего речевого продукта в целом лицо, обладающее специальными знаниями, может обнаружить использование маскировки слов наркотического дискурса.

Например, нередко для маскировки используются лексемы с семантическим полем «продукты питания». Согласно словарным данным наркотического сленга, масло — это концентрированная настойка опия; молоко — отвар дикорастущей конопли в молоке; пшено — папиросы с анашой или гашишем[11].

В своей работе А. Г. Данилин приводит примеры фраз, которые встречаются в разговорах при обсуждении наркотических средств: «Хочу нашего молока», «Мне нужно немного белого хлеба»[12].

[11] Наркоманский словарь Баяна Ширянова // URL: http://imperium.lenin.ru/EOWN/eown7/dictionary/dictionary.html (дата обращения: 15.01.2024).

[12] *Данилин А. Г.* LSD. Галлюциногены, психоделия и феномен зависимости. М. : Центрполиграф, 2001. С. 209.

Несмотря на изменение способов совершения преступлений, связанных с незаконным оборотом наркотических средств, приведенная А. Г. Данилиным лексика всё еще широко используется наркопреступниками.

Анализ показывает, что еще одним вариантом маскировки является внедрение гиперссылок в текст. Причем такие гиперссылки могут не отличаться визуально от других слов в речевом продукте. В таких случаях необходимо привлекать специалиста, который владеет навыками обнаружения скрытых гиперссылок.

Следующая проблема, с которой можно столкнуться на практике при работе с мессенджерами, заключается в появлении секретных чатов. В частности, такая функция предусмотрена в «Телеграме», который наиболее активно используется наркопреступниками.

Особенность секретного чата «Телеграма» состоит в возможности автоматического удаления сообщений по истечении заданного заранее времени (от одной секунды до одной недели) без возможности восстановления. Соответственно, криминалистически значимая информация может быть удалена еще до ее обнаружения.

С учетом этого факта, а также того, что управлять чатами «Телеграма» можно с различных устройств, вероятность потери криминалистически значимой информации возрастает.

При этом информация, которая может содержаться в социальных сетях, мессенджерах, нередко является важной и ключевой для расследования и раскрытия преступлений.

В практике США известен случай, когда по опубликованной фотографии удалось найти поставщика наркотических средств. В рамках операции «Темное золото» сотрудники правоохранительных органов просматривали данные онлайн-магазинов Даркнета. На одном из таких сайтов были опубликованы фотографии, представляющие собой изображение марихуаны на ладони человека. Ввиду того что фотографии были сделаны в высоком разрешении, четко просматривались папиллярные узоры пальцев рук. Данный фотоматериал был направлен на дактилоскопическую экспертизу, в результате которой было обнаружено, что в базе данных уже присутствуют исследуемые отпечатки, принадлежащие Хосе Роберту Поррасу. Таким образом была выявлена личность преступника[13].

Однако для того, чтобы обнаруженные цифровые следы не теряли своей значимости, необходимо обеспечить сохранность имеющихся данных.

Если брать в пример «Телеграм», то в первую очередь нужно завершить сеансы на других устройствах с целью недопущения дистанционного удаления чатов и иной информации.

После этого шага можно, собственно, приступать к работе с цифровыми следами.

Уже были отмечены сложности обнаружения цифровых следов, связанные с маскировками. Однако сто́ит констатировать, что достаточно часто при работе с цифровыми следами специалисты имеют дело с большим объемом информации, что, естественно, требует времени. А при собирании цифровых следов оперативность играет одну из значимых ролей.

В зарубежных странах для ускорения процесса с получением максимального результата начали использовать ряд программ. Например, Cellebrite Pathfinder — это программа, основанная на алгоритмах машинного обучения. Cellebrite Pathfinder автоматически объединяет большие объемы разрозненных источников данных мобильных, облачных, компьютерных и телекоммуникационных сетей с целью выявления необходимой для правоохранительных органов информации[14].

Программа имеет возможности распознавания, обработки и анализа текста, обнаружения фото-, видеоизображений, относящихся к заданной категории (в частности, в категории «наркотические средства»). Не менее важным является

[13] Отчет по результатам проведенной сотрудниками правоохранительных органов США операции «Темное золото» // URL: https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35 (дата обращения: 23.01.2024).

[14] Данные о программе Cellebrite Pathfinder // URL: https://www.dataexpert.eu/products/mobile-forensics-cellebrite/cellebrite-pathfinder/ (дата обращения: 23.01.2024).

способность Cellebrite Pathfinder к получению данных о местонахождении подозреваемых лиц, обнаружению «горячих» точек. С помощью такой программы можно выстраивать в дальнейшем связи и закономерности передвижения, коммуникации лиц, участвующих в наркопреступлениях.

Безусловно, внедрение таких технологий требует проведения ряда масштабных процедур по проверке их функционирования, по их стандартизации, паспортизации. Однако современные проблемы требуют современных решений. И при собирании цифровых следов нельзя обойтись без использования передовых технологий.

В целом весь указанный алгоритм действий применим ко всем мессенджерам, социальным сетям, а также к отдельным приложениям.

При расследовании дел, связанных с незаконным оборотом наркотических средств, наибольшее внимание уделяется именно данным социальных сетей, мессенджеров и сайтов сетей Интернет, Даркнет. При этом не менее криминалистически значимая информация может содержаться в приложениях.

В приговоре от 26.07.2023 по делу № 1-188/2023 Шатурского городского суда Московской области приводятся обстоятельства, согласно которым гражданин А. оборудовал тайники с закладками, используя мобильное приложение «Мэпс.ми». Впоследствии при осмотре его мобильного телефона были найдены «скриншоты из приложения “Мэпс.ми” с географическими координатами местности в количестве 60 штук». При проверке следственно-оперативной группой данных координат были найдены 53 тайника с закладками[15].

Обнаружение данных банковских приложений может позволить отследить историю совершенных операций и, что не менее значимо, получателя денежных средств. Конечно, наркопреступники нередко либо оплачивают наличными, либо прибегают к использованию криптовалюты. И всё же нельзя исключать возможность отслеживаемой бесконтактной оплаты и не проверять данную информацию.

Шпаковский районный суд Ставропольского края в вынесенном им приговоре от 19.07.2023 по делу № 1-187/2023 излагает следующие обстоятельства: гражданин А., используя личный мобильный телефон, через сайт интернет-магазина оформил заказ: «с целью личного потребления? пирролидиновалерофенон, который является производным наркотического средства N-метилэфедрона, в крупном размере». Оплату заказа стоимостью 2 636 руб. гражданин А. провел бесконтактным способом[16].

Приведенные примеры свидетельствуют о том, что данные приложений тоже могут содержать в себе криминалистически значимую информацию, которая при соблюдении всех процессуальных норм может стать в дальнейшем доказательством.

Не раз отмечалось, что цифровые следы неотделимы от их носителей, поэтому изъятию подлежат непосредственно носители.

В случае, когда носителем является мобильный телефон, планшет, необходимо иметь в виду, что если устройство находится во включенном состоянии, то команды дистанционного уничтожения информации могут быть применены без ведома следователя. Некоторые устройства имеют автоматический таймер для включения телефона с целью обновления, что также может поставить под угрозу данные, поэтому оптимальный вариант — извлечение аккумулятора.

Если устройство невозможно выключить, его необходимо изолировать от вышки сотовой связи, поместив в сумку Фарадея или другой блокирующий материал, перевести в режим полета либо отключить Wi-Fi, Bluetooth или другую систему связи. Цифровые устройства следует помещать в антистатическую упаковку, например в бумажные пакеты или конверты и картонные коробки. Следует избегать пластика, поскольку он может передавать статическое электриче-

[15] Приговор от 26.07.2023 по делу № 1-188/2023 Шатурского городского суда Московской области // URL: https://sudact.ru/regular/doc/7CPamAaBkmmJ/ (дата обращения: 20.01.2024).

[16] Приговор от 19.07.2023 по делу № 1-187/2023 Шпаковского районного суда Ставропольского края // URL: https://sudact.ru/regular/doc/DSn8SXFf2qg9/ (дата обращения: 20.01.2024).

ство, способствовать накоплению конденсата или влажности.

Изъятие компьютера — более сложный процесс. В каждом случае необходимо учитывать существующие особенности, например, включен или выключен был компьютер при его обнаружении, подключен ли компьютер к локальной сети и даже в рамках какого невербального следственного действия происходит изъятие носителя.

В науке уже выработаны рекомендации по обращению с цифровыми следами при их обнаружении, фиксации и изъятии. Однако теперь необходимо разработать методику, которая бы стандартизировала положения относительно порядка работы с цифровыми следами.

Важно отметить, что при выключении компьютера значимая информация может быть утеряна. Но в ситуации, когда на включенном компьютере запущена программа, форматирующая, удаляющая информацию, необходимо немедленно отключить питание компьютера, чтобы сохранить оставшиеся на нем данные.

Вне зависимости от того, с каким носителем специалист имеет дело, он должен четко и полно отражать «в протоколе манипуляции, производимые как с осматриваемыми физическими объектами (средствами вычислительной техники, электронными носителями информации), так и непосредственно с объектами информационными»[17].

Через фиксацию дополнительно обеспечивается сохранность цифровых следов и их носителей, с помощью фиксации можно отследить, каким образом были обнаружены и изъяты цифровые следы.

Действия специалиста фиксируются в протоколе следственного действия, который в дальнейшем исследуется в суде. И, к сожалению, не всегда такая фиксация проводится в нужном порядке.

В частности, в приговоре от 09.06.2023 по делу № 1-120/2023 Ярославского районного суда отражено, что на определенном сайте интернет-магазина подсудимым были приобретены семена конопли, а также изучены посредством сети «Интернет» способы, методы и основы выращивания конопли[18].

Изложенные факты, исходя из текста приговора, подтверждаются исключительно показаниями подсудимого. Однако из-за отсутствия привлечения специалиста возникают вопросы: с какого носителя совершались подсудимым указанные в приговоре действия? точно ли именно подсудимый пользовался данными устройствами, заходил в сеть и осуществлял ряд операций?

Во всех обозначенных аспектах собирания цифровых следов прослеживается необходимость участия специалиста, который бы смог обеспечить сохранность цифровых следов. Именно специалист владеет знаниями о том, какие методы и в каком порядке нужно применять в каждом конкретном случае, что необходимо фиксировать в протоколах следственных действий, какая информация является значимой.

В законодательстве участие специалиста по изъятию электронных носителей в следственных действиях регулируется статьей 164.1 УПК РФ[19]. Однако этой статьей не охватываются все вопросы, возникающие при работе с цифровыми следами и требующие правового регулирования.

Если обращаться к опыту зарубежных стран, а именно США, то, как указывает Национальный институт юстиции, собиранием цифровых следов должны заниматься лица, обладающие специальными знаниями, иначе говоря, специалисты[20].

---

[17] *Россинская Е. Р.*, *Рядовский И. А.* Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex russica. 2021. Т. 74. № 9. С. 107.

[18] Приговор от 09.06.2023 по делу № 1-120/2023 Ярославского районного суда // URL: https://sudact.ru/regular/doc/fnQtVFPisVbb/ (дата обращения: 20.01.2024).

[19] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 14.02.2024) // URL: https://www.consultant.ru/document/cons_doc_LAW_34481/a181248bd35e283bbf253a905940bfb32dd9923e/ (дата обращения: 20.01.2024).

[20] Electronic Crime Scene Investigation : A Guide for First Responders / National Institute of Justice (2008, April). Second edition // URL: https://nij.ojp.gov/library/publications/electronic-crime-scene-investigation-guide-first-responders-second-edition (дата обращения: 20.01.2024).

Действительно, компетенций следователя уже на данный момент будет недостаточно для эффективной работы с современными технологиями.

Нельзя преуменьшать важность производства отдельных следственных действий с участием специалиста, особенно в категории дел, связанных с незаконным оборотом наркотических средств в компьютерных сетях. Их специфика априори предполагает необходимость привлечения лиц, обладающих специальными знаниями в определенной области.

БИБЛИОГРАФИЯ

1. *Аверьянова Т. В.*, *Белкин Р. С.*, *Корухов Ю. Г.*, *Россинская Е. Р.* Криминалистика : учебник для вузов. — 4-е изд., перераб. и доп. — М. : Норма : Инфра-М, 2014. — 928 с.
2. *Вехов В. Б., Смагоринский Б. П., Ковалев С. А.* Электронные следы в системе криминалистики // Судебная экспертиза. — 2016. — Вып. 2. — С. 10–19.
3. *Данилин А. Г.* LSD. Галлюциногены, психоделия и феномен зависимости. — М. : Центрполиграф, 2001. — 521 с.
4. *Дерюгин Р. А.*, *Жижелева А. А.* Перспективы развития цифровой криминалистики в условиях информационного общества // Технологии XXI века в юриспруденции : материалы Всероссийской научно-практической конференции (Екатеринбург, 24–25 мая 2019 г.) / под ред. Д. В. Бахтеева. — С. 40–46.
5. *Мещеряков В. А.* Преступления в сфере компьютерной информации: основы теории и практики расследования. — Воронеж : Изд-во Воронежского государственного университета, 2002. — 408 с.
6. *Россинская Е. Р.*, *Рядовский И. А.* Тактика и технология производства невербальных следственных действий по делам о компьютерных преступлениях: теория и практика // Lex russica. — 2021. — Т. 74. — № 9. — С. 102–118.
7. *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.
8. Теория информационно-компьютерного обеспечения криминалистической деятельности : монография / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский ; под ред. Е. Р. Россинской. — М. : Проспект, 2022. — 254 с.

Материал поступил в редакцию 11 марта 2024 г.

REFERENCES (TRANSLITERATION)

1. Averyanova T. V., Belkin R. S., Korukhov Yu. G., Rossinskaya E. R. Kriminalistika: uchebnik dlya vuzov. — 4-e izd., pererab. i dop. — M.: Norma: Infra-M, 2014. — 928 s.
2. Vekhov V. B., Smagorinskiy B. P., Kovalev S. A. Elektronnye sledy v sisteme kriminalistiki // Sudebnaya ekspertiza. — 2016. — Vyp. 2. — S. 10–19.
3. Danilin A. G. LSD. Gallyutsinogeny, psikhodeliya i fenomen zavisimosti. — M.: Tsentrpoligraf, 2001. — 521 s.
4. Deryugin R. A., Zhizheleva A. A. Perspektivy razvitiya tsifrovoy kriminalistiki v usloviyakh informatsionnogo obshchestva // Tekhnologii XXI veka v yurisprudentsii: materialy Vserossiyskoy nauchno-prakticheskoy konferentsii (Ekaterinburg, 24–25 maya 2019 g.) / pod red. D. V. Bakhteeva. — S. 40–46.
5. Meshcheryakov V. A. Prestupleniya v sfere kompyuternoy informatsii: osnovy teorii i praktiki rassledovaniya. — Voronezh: Izd-vo Voronezhskogo gosudarstvennogo universiteta, 2002. — 408 s.

6. Rossinskaya E. R., Ryadovskiy I. A. Taktika i tekhnologiya proizvodstva neverbalnykh sledstvennykh deystviy po delam o kompyuternykh prestupleniyakh: teoriya i praktika // Lex russica. — 2021. — T. 74. — № 9. — S. 102–118.
7. Rossinskaya E. R. Teoriya informatsionno-kompyuternogo obespecheniya kriminalisticheskoy deyatelnosti: kontseptsiya, sistema, osnovnye zakonomernosti // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. — 2019. — № 2 (89). — S. 193–202.
8. Teoriya informatsionno-kompyuternogo obespecheniya kriminalisticheskoy deyatelnosti: monografiya / E. R. Rossinskaya, A. I. Semikalenova, I. A. Ryadovskiy; pod red. E. R. Rossinskoy. — M.: Prospekt, 2022. — 254 s.