Научная статья
УДК 343.9
DOI 10.33184/vest-law-bsu-2025.27.23

Харисова Зарина Ирековна
Уфимский университет науки и технологий, Уфа, Россия,
zarinaid@mail.ru, https://orcid.org/0000-0002-3902-3459

ПРОГРАММНЫЕ ТЕХНИКО-КРИМИНАЛИСТИЧЕСКИЕ СРЕДСТВА КАК ОСНОВА СОВРЕМЕННОЙ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. В статье представлен комплексный обзор имеющихся на сегодняшний день программных технико-криминалистических средств, обеспечивающих наиболее эффективное собирание, фиксацию, изъятие и исследование цифровых доказательств. Сделан вывод, что в условиях цифровизации общества рассматриваемое программное обеспечение приобретает стратегическое значение в борьбе с преступлениями в сфере компьютерной информации, обеспечивая в автоматизированном виде помимо фиксации верификацию цифровых данных, проверку их подлинности и сохранности, восстановление удаленных и зашифрованных сведений, выдачу прогнозов и рекомендаций по расследованию, а также удобство и оперативность обработки больших массивов данных за счет использования технологий машинного обучения, распознавания текстовых, графических и биометрических данных. Показано, что только программные технико-криминалистические средства смогут обеспечить эффективное противодействие атакам, управляемым искусственным интеллектом в будущем, что подчеркивает насущность их рассмотрения в настоящее время.

Ключевые слова: компьютерные преступления, киберпреступления, технико-криминалистическое средство, программное обеспечение, цифровая криминалистика, расследование киберпреступлений, искусственный интеллект, анализ данных

Для цитирования: Харисова З.И. Программные технико-криминалистические средства как основа современной методики расследования преступлений в сфере компьютерной информации / З.И. Харисова. – DOI 10.33184/vest-law-bsu-2025.27.23 // Вестник Института права Башкирского государственного университета. – 2025. – № 3. – С. 237–250.

Original article

Kharisova Zarina Irekovna
Ufa University of Science and Technologies, Ufa, Russia, zarinaid@mail.ru,
https://orcid.org/0000-0002-3902-3459

SOFTWARE FORENSIC EQUIPMENT AS THE BASIS FOR MODERN METHODS TO INVESTIGATE CYBERCRIME

Abstract: The article provides a comprehensive overview of the software forensic equipment available to date that provide the most effective collection, recording, seizure and examination of digital evidence. It was concluded that in the context of the society digitalisation, the software in question acquires strategic importance in the fight against crimes in the cyber realm, providing in an automated form, in addition to fixing, verification of digital data, verification of their authenticity and safety, recovery of deleted and encrypted data, issuance of forecasts and recommendations for investigation, as well as convenience and efficiency of processing large amounts of data through the use of machine learning technologies, authorisation of text, graphic and biometric data. It is shown that only software forensic equipment will be able to provide an effective response to attacks controlled by artificial intelligence in the future, which underlines the urgency of their consideration at present.

Keywords: computer crimes, cybercrimes, software forensic equipment, software, digital forensics, cybercrime investigation, artificial intelligence, data analysis

For citation: Kharisova Z.I. Software Forensic Equipment as the Basis for Modern Methods to Investigate Cybercrime. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta = Bulletin of the Institute of Law of the Bashkir State University,* 2025, no. 3, pp. 237–250. (In Russian). DOI 10.33184/vest-law-bsu-2025.27.23.

Введение. С точки зрения уголовно-процессуального законодательства поиск, фиксация и изъятие цифровых следов производятся в ходе таких следственных действий как следственный осмотр, обыск и выемка, при которых непосредственно компьютерную информацию невозможно изъять, но можно осуществить ее копирование. Чтобы эффективно провести собирание, фиксацию, оценку или копирование цифровых доказательств необходимо не только наличие специальных знаний, но и применение специальных технических средств. В целях снижения временных и трудовых затрат при расследовании преступлений в сфере компьютерной информации, неоправданного назначения компьютерно-технических экспертиз, важно понимать, где и какие цифровые доказательства целесообразно искать, как их фиксировать и, соответственно, с помощью каких средств осуществлять их копирование и последующую оценку.

С целью подтверждения вышеуказанного необходимо рассмотреть особенности фиксации цифровых доказательств на электронных носителях данных и возможности расследования преступлений в сфере компьютерной информации с применением программных технико-криминалистических средств в виде отечественных и зарубежных решений.

Особенности фиксации цифровых доказательств на электронных носителях информации. Обнаружение цифровых следов преступлений является поисковой деятельностью следователя, которая направлена на собирание доказательственной и ориентирующей криминалистически значимой информации, что возможно с использованием различных технических устройств (компьютерных, мобильных и пр.), а также программных технико-криминалистических средств. Под фиксацией цифровых доказательства предполагается сохранение фактических данных, находящихся в электронной форме, которое осуществляется в следующем порядке [1, с. 108]:

производится трансформация доказательственных электронных данных, содержащихся на электронном носителе информации, в форму, доступную для восприятия ее человеком;

устанавливаются сведения о носителе информации, на котором найдена криминалистически значимая компьютерная информация, владелец носителя, возможность передачи данных, хранящихся на нем, операционная система устройства с установленным накопителем, файлы и каталоги данных, в которых найдены доказательства, а также сведения об их создании или изменении;

обеспечивается фильтрация значимых данных о событии преступления из массива всех имеющихся сведений на носителе информации, выявление способов их получения, а также сохранение доказательственной информации для неоднократного ее использования в процессе доказывания, например, в процессе судебно-экспертного исследования, предъявления как доказательства в ходе допроса и т. д. [2, с. 18] путем фотографирования (формирования скриншота) экрана с выведенной криминалистически значимой компьютерной информацией;

криминалистически значимая компьютерная информация изымается вместе с носителем информации, либо создается клон носителя, в случае, когда его изъятие невозможно или нецелесообразно.

Цифровые доказательства находятся в сложных формах, обусловленных структурой носителя информации [3, с. 41], соответственно, работа с ними осуществляется в рамках процессуальных действий, к производству которых, как правило, привлекаются специалисты. Так, в соответствии с ч. 2 ст. 164.1 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), при производстве обыска или выемки, в ходе которых планируется изъятие компьютеров или иных носителей компьютерной информации, необходимо участие специалиста, обладающего специальными знаниями в области компьютерной техники, средств связи и передачи цифровой информации [4, с. 170]. Носителем компьютерных данных на международном уровне признается электронный но-

ситель информации, представляющий из себя любой предмет или материал, с которого можно воспроизводить информацию с помощью или без помощи какого-либо устройства[1]. Действующая в настоящее время процедура изъятия носителя информации сопряжена с рядом трудностей и не всегда обеспечивает достаточную эффективность, а допустимость электронных доказательств в значительной степени определяется участием при обыске и выемке компьютерной информации специалиста. Однако данный факт все чаще вызывает сложности у практических работников и обширные дискуссии в научных кругах[2]. Сторонники обязательного привлечения специалиста указывают на его роль в предотвращении утраты или искажения изымаемой информации [5, с. 81; 6, с. 23; 7, с. 82]. Ряд исследователей считают требование, закрепленное ч. 2 ст. 164.1 УПК РФ, избыточным [8, с. 66; 9, с. 18; 10, с. 13], аргументируя это ограничением процессуальной самостоятельности следователя, усложнением организационных мероприятий при подготовке и проведении следственных действий, увеличением затрачиваемого на уголовное судопроизводство времени. Придерживаясь второй позиции, необходимо отметить, что имеется ряд ситуаций, когда участие специалиста безусловно обязательно, например, в случае изъятия энергозависимых носителей или вмешательства в конструкцию сложных технических средств. При этом очевидно, что при изъятии съемных носителей информации участие специалиста не требуется, поскольку достаточно лишь их герметичного упаковывания.

Сложность исследования электронных носителей информации зависит от его вида. Наиболее просты в работе объекты, не имеющие функций, ограничивающих к ним доступ, в отличие от мобильных средств связи [11, с. 2] и компьютеров. Стоит отметить также сложности, возникающие при осмотре IoT-устройств, а также удаленно расположенных носителей данных (веб-ресурсов), облачных хранилищ, распределенных реестров, аппаратных криптокошельков [12, с. 72], сетей с туннелированием [13, с. 105] и т. п. объектов и сред, которые могут потребовать участия в раскрытии и расследовании не только специалистов Управления по организации борьбы с противоправным использованием информационно-телекоммуникационных технологий, но и дополнительного привлечения сотрудников специализированных компаний в сфере информаци-

---

[1] National Cybercrime Strategy : Guidebook (Национальная стратегия борьбы с киберпреступностью: руководство) [Электронный ресурс] // Официальный сайт Международной организации уголовной полиции (Интерпол). URL: https://www.interpol.int/content/download/16455 /file/Cyber_Strategy_Guidebook.pdf (дата обращения: 25.06.2025).

[2] Flander, B. Erbeznik, A. Toolkit for handling and admissibility of electronic evidence empowering legal practitioners to critically. Review electronic evidence from the procedural rights perspective [Электронный ресурс] // Официальный сайт научно-исследовательского центра «ZRS Koper» (Словения). URL: https://www.zrs-kp.si/wp-content/uploads/2024/07/innocent_monografija_online_edition.pdf (дата обращения: 25.06.2025).

онных технологий. Кроме того, требование участия специалиста при производстве копирования изымаемой информации в ходе производства следственных действий представляется оправданным, поскольку это объясняется необходимостью отождествления изъятой и скопированной информации. По этой причине предполагается рациональным закрепление за следователем права, но не обязанности привлечения специалиста при изъятии электронных носителей информации, исходя из собственных компетенций [14, с. 420] (в зависимости от реальной необходимости в использовании специальных знаний при проведении следственных действий). Если в ходе следственных действий не проводится исследование информации, содержащейся на носителе, как, например, в случае его осмотра или копирования информации, то решение вопроса об участии специалиста вполне может осуществляться следователем (дознавателем) самостоятельно в порядке, предусмотренном ст. 168 УПК РФ [15, с. 48].

Обращение с простыми электронными носителями информации, например, USB-накопителями, является на сегодняшний день бытовым навыком [16, с. 67], по этой причине, целесообразным представляется следующее дополнение ч. 2 ст. 164.1 УПК РФ: «Энергозависимые электронные носители информации подлежат изъятию с обязательным участием специалиста. В иных случаях специалист привлекается по усмотрению следователя при отсутствии у последнего компетенций, исключающих риск повреждения, модификации или уничтожения данных. Изъятие или копирование информации сопровождается видеозаписью, за исключением ситуаций изъятия энергонезависимых носителей без исследования их содержимого».

Рассматриваемая проблема также требует учета современных технологических вызовов, включая распространение облачных хранилищ и IoT-устройств, не подпадающих под традиционное понимание электронного носителя информации и совершенствования системы подготовки следователей в области цифровой криминалистики. Дополнительно следует рассмотреть вопрос о разработке рекомендаций по изъятию цифровых доказательств, адаптируемых к изменяющимся условиям технического прогресса, а также провести комплексный обзор существующих в настоящее время программных технико-криминалистических средств, которые можно использовать при расследовании преступлений в сфере компьютерной информации.

Отечественные и зарубежные технико-криминалистические средства, используемые при расследовании преступлений в сфере компьютерной информации. Так, в отношении неправомерного доступа к компьютерной информации (ст. 272 УК РФ) программные технико-криминалистические средства позволяют автоматизировать собирание доказательств, проводить анализ носителей данных (программное обеспечение «Мобильный криминалист (десктоп,

эксперт, эксперт плюс)»[3], «Elcomsoft Premium Forensic Bundle»[4], «Sleuth Kit», «Autopsy», «Caine», «HDDScan» и пр.), исследовать метаданные («jExifToolGUI», «Metadata», «ExifTool» и др.), идентифицировать факт несанкционированного доступа («SQL Forensics», «DB Shield» и пр.), восстановить удаленную информацию («EnCase» и «FTK Forensic Toolkit», «PC-3000»[5]), зафиксировать сетевой трафик (программное обеспечение «TcpDump», «Wireshark», «Zeek»), а также сформировать журнал событий и активности злоумышленника («IBM QRadar», «Splunk» и др.). Использование указанного программного обеспечения позволяет автоматизировать и ускорить поиск и исследование цифровых доказательств, сводя к минимуму человеческий фактор. Тем не менее, интерпретация полученных данных зачастую требует экспертных знаний, что во многом зависит от полноты исходных данных по делу.

В рамках расследования незаконного использования, передачи, сбора и хранения компьютерной информации, содержащей персональные данные граждан (272.1 УК РФ), программные технико-криминалистические средства могут обеспечивать фиксацию утечек конфиденциальных сведений (программное обеспечение «Maltego», «SpiderFoot», «Symantec Data Loss Prevention», «Have I Been Pwned» и др.), в том числе запрещенных к распространению данных (поисковая система «Seus»)[6], выявление маршрутов передачи данных («Wireshark» и др.), мониторинг трафика, в том числе выявление продаж баз данных с персональными данными в сети даркнет («Darknet Tracer», «CipherTrace» и пр.), и предотвращение утечек информации

[3] Программное обеспечение «Мобильный Криминалист Эксперт Плюс» [Электронный ресурс] // Официальный сайт Единого реестра российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://reestr.digital.gov.ru/reestr/423110/?sphrase_id=5937674 (дата обращения: 25.06.2025 г.).

[4] Программное обеспечение «Elcomsoft Premium Forensic Bundle» [Электронный ресурс] // Официальный сайт Единого реестра российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://reestr.digital.gov.ru/reestr/436808/?sphrase_id=5929589 (дата обращения: 25.06.2025 г.).

[5] Программное обеспечение «PC-3000 Portable» [Электронный ресурс] // Официальный сайт Единого реестра российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://reestr.digital.gov.ru/reestr/310277/?sphrase_id=5929598 (дата обращения: 25.06.2025 г.).

[6] Программное обеспечение «Поисковая система SEUS» [Электронный ресурс] // Официальный сайт Единого реестра российских программ для электронных вычислительных машин и баз данных Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://reestr.digital.gov.ru/reestr/305124/?sphrase_id=5929711 (дата обращения: 25.06.2025 г.).

(DLP-системы (от англ. «Data Loss Prevention» – предотвращение утечки данных) Symantec, InfoWatch и пр.). Преимуществами использования указанного программного обеспечения являются возможность анализа значительных объемов данных, мониторинга подозрительной активности в реальном времени, высокая эффективность выявления мест хранения скомпрометированных данных, автоматизация поиска утечек конфиденциальных сведений на теневых рынках. При этом недостатками являются высокая вычислительная нагрузка, вероятность ошибок при автоматизированном анализе, а также риск нарушения конфиденциальности при обработке персональных данных.

В отношении создания, использования и распространения вредоносного программного обеспечения (ст. 273 УК РФ) программные технико-криминалистические средства позволяют исследовать вредоносный код, например, идентифицируя способы его распространения и алгоритмы исполнения (программное обеспечение «IDA Pro», «OllyDbg», «Ghidra», «VirusTotal» и пр.), проводить динамический анализ и эмуляцию поведения вирусов («Cuckoo Sandbox», «Any.Run» и пр.), фильтровать подозрительный трафик («Snort», «Suricata» и пр.) и фиксировать вредоносную активность («Kaspersky», «Symantec», «McAfee» и пр.). Преимуществами использования вышеуказанных средств являются высокая точность в определении функционала вредоносных программ, обновляемые базы данных сигнатур, автоматизированное обнаружение новых угроз и возможность отслеживания цепочек их распространения.

В целях обнаружения нарушений правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) используются программные технико-криминалистические средства: средства, фиксирующие действия пользователей и системных администраторов (программное обеспечение «QRadar», «ArcSight» и пр.); средства централизованного мониторинга нарушений требований информационной безопасности и фактов несанкционированного доступа или неправильной эксплуатации программного обеспечения («Solar Dozor», «Snort», «Suricata» и пр.); средства выявления уязвимостей в сетевых устройствах («Nessus», «OpenVAS»), средства анализа журналов событий и изменения программ («AlienVault», «ArcSight», «Graylog», «LogRhythm» и пр.). Несмотря на все преимущества использования указанных средств и возможность предотвращения инцидентов информационной безопасности общим их недостатком являются трудоемкость сбора и интерпретации данных. В целях выяснения обстоятельств, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), программные технико-криминалистические средства также позволяют осуществлять мониторинг и анализ сетевого трафика, отслеживание производительности сети (программное обеспечение «Wireshark», «Network Miner», «SolarWinds Network Performance Monitor»), обнаруживать вредоносную активность («IDA Pro», «OllyDbg»,

«Ghidra», «VirusTotal» и пр.), восстанавливать удаленные или поврежденные данных с носителей информации с последующим их анализом («Elcomsoft Premium Forensic Bundle», «PC-3000», «Sleuth Kit», «Autopsy», «Caine», «HDDScan» и пр.), исследовать метаданные («jExifToolGUI», «Metadata», «ExifTool» и др.), проводить аудит управления учетными записями (средства автоматизации управления доступом «IDM» (от англ. «identity management» – управление идентификацией), «IAM» (от англ. (identity and access management» – управление идентификацией и доступом) и «IGA» (от англ. «identity governance & administration» – управление идентификацией и ее администрированием), а также формировать журнал событий и активности злоумышленника («IBM QRadar», «Splunk» и др.). Помимо указанного непосредственно субъектами критической информационной инфраструктуры Российской Федерации, может применяться иное вспомогательное программное обеспечение, позволяющее идентифицировать нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также расследовать инциденты информационной безопасности.

В отношении неправомерного воздействия на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1 УК РФ) программные технико-криминалистические средства, например, могут обеспечить обнаружение атак на промышленные системы (программное обеспечение «Wireshark», «Tofino Xenon», «Radiflow», «Nozomi Networks» и пр.), мониторинг сетевого трафика и выявление аномалий в режиме реального времени («Splunk», «ELK Stack», «NetFlow» и пр.), анализ трафика и журналов событий («IBM X-Force», «FireEye» и пр.).

В целях выявления нарушений правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ) программные средства могут позволить, например, выявлять нарушения при управлении интернет-трафиком (программное обеспечение «Суверенный Рунет», «NetWitness», «Deep Packet Inspection», «BGPmon», «RIPEstat» и пр.), проводить аудит управления учетными записями (средства автоматизации управления доступом «IDM», «IAM» и «IGA»), проводить расследования инцидентов и отслеживать запрещенные ресурсы, контролировать доступ к ресурсам («Ревизор», «FireEye SORM», «Farsight Security», «Cisco Umbrella», «Palo Alto» и пр.).

Таким образом, применение специализированных программных технико-криминалистических средств является основой современной методики расследования преступлений в сфере компьютерной информации, которая обеспечивает оперативное выявление и анализ инцидентов в режиме реального времени, восстановление и реконструкцию цифровых следов с высокой точностью,

интеграцию данных из различных источников и уровней инфраструктуры. Приведенный перечень средств не является исчерпывающим, однако позволяет показать широту их потенциала в расследовании преступлений в сфере компьютерной информации.

Стоит также отметить, что на сегодняшний день в работе органов внутренних дел широко применяются сервисы обеспечения повседневной и оперативно-служебной деятельности системы ИСОД МВД России, а также различные информационные системы поискового и экспертного назначения. Однако стоит отметить сложившийся недостаток оснащения техническими средствами [17, с. 206], которые позволяют иметь конкурентное преимущество в борьбе с преступностью, что снижает эффективность деятельности органов внутренних дел по расследованию, раскрытию и предотвращению преступных деяний. Оптимизации сроков осуществления следственных действий и иных процессуальных действий, направленных на установление обстоятельств, входящих в предмет доказывания, будет способствовать закрепление в уголовно-процессуальном законодательстве более четких оснований и процессуальных регламентов, регулирующих собирание цифровых доказательств с применением информационных технологий и программных технико-криминалистических средств.

Соответственно, можно сделать вывод, что в условиях цифровизации общества программные технико-криминалистические средства приобретают стратегическое значение в борьбе с преступностью, обеспечивая, во-первых, непосредственное собирание, фиксацию, изъятие и исследование цифровых доказательств (за счет использования экспертных и поисковых систем), во-вторых, их верификацию и проверку подлинности и сохранности (например, за счет использования алгоритмов хеширования для создания контрольных сумм цифровых объектов и последующей проверки их неизменности), в-третьих, восстановление удаленных и зашифрованных данных (например, за счет применения методов цифровой стеганографии или интеграции блокчейн-технологий), а также удобство и оперативность обработки больших массивов разнородной информации (за счет использования технологий машинного обучения и хранения данных в распределенных реестрах, распознавания текстовых, графических и биометрических данных и пр.), выдачи прогнозов и рекомендаций (на базе предиктивного анализа и корреляции данных).

В настоящее время в свободном доступе имеется разнообразное программное обеспечение для поиска, анализа и интерпретации цифровых доказательств, однако его применение сотрудниками органов внутренних дел ограничено в силу отсутствия четкого нормативного регулирования. Так, на примере OSINT-инструментов для поиска информации из открытых источников можно констатировать, что в силу действующего законодательства применение подобного метода сбора данных возможно лишь при наличии судебного решения, однако даже в этом случае возникают риски нарушения конституционных прав граждан, включая неприкосновенность частной жизни, личную и семей-

ную тайну, а также тайну переписки. Соответственно, для эффективного выявления и пресечения преступной деятельности в сфере компьютерной информации необходима правовая регламентация применения программных технико-криминалистических средств, обеспечивающая баланс между возможностями правоохранительных органов и соблюдением конституционных прав граждан.

Поскольку предполагаемым вектором развития киберпреступности является использование различных генеративных алгоритмов машинного обучения, соответственно, для противодействия таким угрозам необходимы программные средства, способные самостоятельно, на основе гибких алгоритмов искусственного интеллекта, без участия человека, например, идентифицировать аномалии в сетевом трафике, анализировать вредоносный код и, соответственно, адаптироваться к новым видам атак. Определенную трудность будет также представлять появление квантовых компьютеров, способных взламывать современные криптографические алгоритмы. Для противодействия этой угрозе программные комплексы цифровой криминалистики должны будут включать гибридные квантовые алгоритмы взлома шифрования, сочетающие традиционные методы криптоанализа с вероятностными вычислениями квантовых систем.

Таким образом, только программные технико-криминалистические средства смогут эффективно бороться с атаками, управляемыми искусственным интеллектом, в будущем, что подчеркивает насущность их рассмотрения в настоящее время.

Заключение. С учетом вышеизложенного можно сделать вывод, что особенности киберсреды исключают применение традиционных технико-криминалистических средств, поскольку цифровые следы не имеют физических характеристик в классическом понимании, являются легко изменяемыми и уничтожаемыми, кроме того, большие массивы цифровой информации зачастую размещены в различных средах и (или) хранилищах, что исключает возможность их ручного анализа. В отличие от традиционных вещественных доказательств, цифровые доказательства требуют специфических подходов к собиранию, хранению и анализу, так как они легко поддаются модификации. Автоматизацию исследования цифровой информации, точность и воспроизводимость результатов ее анализа, обеспечение своевременного собирания и использования криминалистически значимой информации в электронной форме позволяют обеспечить только программные технико-криминалистические средства.

Таким образом, программные технико-криминалистические средства играют ключевую роль в расследовании преступлений в сфере компьютерной информации, что обусловлено предоставляемыми ими возможностями поиска, фиксации, собирания, исследования и хранения криминалистически значимой компьютерной информации.

Список источников

1. Бычков В.В. Электронное следообразование преступной деятельности в сети Интернет / В.В. Бычков // Расследование преступлений: проблемы и пути их решения. – 2020. – № 1 (27). – С. 106–111.

2. Цифровые следы преступлений : монография / А.М. Багмет, В.В. Бычков, С.Ю. Скобелин, Н.Н. Ильин. – Москва : Проспект, 2023. – 168 с.

3. Masmoudi S. Unveiling the Human Factor in Cybercrime and Cybersecurity: Motivations, Behaviors, Vulnerabilities, Mitigation Strategies, and Research Methods / S. Masmoudi // Cybercrime Unveiled: Technologies for Analysing Legal Complexity. – 2025. – V. 1181. – P. 41–91.

4. Курс криминалистики. В 3 т. Т. 3. Методика расследования преступлений в сфере экономической деятельности. Методика расследования преступлений против общественной безопасности, других видов и групп преступлений : учебник / М.А. Григорьева, Н.А. Данилова, С.Г. Евдокимов и др. ; под ред. О.Н. Коршуновой. – 3-е изд. – Санкт-Петербург : Юридический центр Пресс, 2024. – 752 с.

5. Гаврилин Ю.В. Процессуальный порядок собирания доказательств на энергонезависимых локальных электронных носителях информации / Ю.В. Гаврилин, А.А. Балашова // Сибирский юридический вестник. – 2020. – № 2 (89). – С. 77–82.

6. Вехов В.Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства / В.Б. Вехов // Российский следователь. – 2013. – № 10. – С. 22–24.

7. Федулова А.Е. Участие специалиста в производстве следственных действий с электронными носителями информации / А.Е. Федулова // Юридическая наука и правоохранительная практика. – 2023. – № 1 (63). – С. 80–87.

8. Шигуров А.В. Новеллы и проблемы правового регулирования порядка проведения следственных действий, связанных с изъятием электронных носителей информации / А.В. Шигуров // Гуманитарные и политико-правовые исследования. – 2021. – № 2 (13). – С. 64–73.

9. Козловский П.В. Участие специалиста в изъятии электронных носителей / П.В. Козловский, П.В. Седельников // Научный вестник Омской академии МВД России. – 2014. – № 1 (52). – С. 17–19.

10. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании : автореф. дис. ... канд. юрид. наук : 12.00.09 / А.А. Балашова. – Москва, 2020. – 30 с.

11. Jian X. Towards a Joint Semantic Analysis in Mobile Forensics Environments / X. Jian, M. Siegel, D. Labudde, M. Spranger // Forensic Science International: Digital Investigation. – 2025. – V. 52 (3):301846. – P. 1–26.

12. Тисен О.Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О.Н. Тисен // Уголовное право. – 2024. – № 3. – С. 69–80.

13. Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений / А.Б. Смушкин // Актуальные проблемы российского права. – 2022. – Т. 17, № 3. – С. 102–111.

14. Мещеряков В.А. К вопросу об оценке компетенции судебного эксперта / В.А. Мещеряков, О.Ю. Цурлуй, Ю.С. Кудрявцев // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции, Москва, 25–26 марта 2021 г. – Москва : Российский государственный университет правосудия, 2021. – С. 417–422.

15. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве / Ю.В. Гаврилин // Труды Академии управления МВД России. – 2017. – № 4 (44). – С. 45–50.

16. Рудаков Б.В. К вопросу о проблемах использования цифровых (электронных) данных в доказывании по уголовным делам / Б.В. Рудаков // Правопорядок: история, теория, практика. – 2021. – № 1 (28). – С. 65–71.

17. Горбунова Е.Ю. Проблемы качества судебно-экспертных исследований (судебная компьютерно-техническая экспертиза) / Е.Ю. Горбунова // Дискуссионные вопросы теории и практики судебной экспертизы : материалы IV Международной научно-практической конференции, Москва, 25–26 марта 2021 г. – Москва : Российский государственный университет правосудия, 2021. – С. 202–207.

References

1. Bychkov V. V. Electronic Tracing of Criminal Activity on the Internet. *Investigation of Crimes: Problems and Solutions*, 2020, no. 1 (27), pp. 106–111. (In Russian).

2. Bagmet A. M., Bychkov V. V., Skobelin S. Yu., Ilyin N. N. Digital Crimes Traces: Monograph. Moscow, Prospect, 2023. 168 p. (In Russian).

3. Masmoudi S. Unveiling the Human Factor in Cybercrime and Cybersecurity: Motivations, Behaviors, Vulnerabilities, Mitigation Strategies, and Research Methods. Cybercrime Unveiled: Technologies for Analysing Legal Complexity, 2025, V. 1181, pp. 41–91. (In English).

4. Korshunova O. N. (ed.). Forensic Science Course: Collection of Scientific Papers: in 3 Volumes. Methodology for Investigating Crimes in the Sphere of Economic Activity. Methodology for Investigating Crimes against Public Safety, Other Types and Groups of Crimes: Textbook. Saint Petersburg, Legal Center Press, 2024. 752p. (In Russian).

5. Gavrilin Yu. V., Balashova A. A. Procedural Procedure for Collecting Evidence on Non–Volatile Local Electronic Media. *Siberian Law Herald*, 2020, no. 2 (89), pp. 77–82. (In Russian).

6. Vekhov V. B. Working with Electronic Evidence in the Context of Changed Criminal Procedure Legislation. *Russian Investigator,* 2013, no. 10, pp. 22–24. (In Russian).

7. Fedulova A. E. Participation of a Specialist in the Process of Conducting of Investigative Actions Involving Electronic Information Carries. *Legal Science and Law Enforcement Practice,* 2023, no 1 (63), pp. 80–87. (In Russian).

8. Shigurov A. V. News and Problems of Legal Regulation of the Procedure for Conducting Investigative Actions Related to Withdrawal of Electronic Media of Information. *Humanitarian and Political-Law Studies*, 2021, no. 2 (13), pp. 64–73. (In Russian).

9. Kozlovsky P. V., Sedelnikov P. V. Specialist's Involvement in Seizing of Electronic Media. *Scientific Bulletin of the Omsk Academy of the Ministry of Interior of Russia,* 2014, no. 1 (52), pp. 17–19. (In Russian).

10. Balashova A. A. Electronic Information Carriers and Their Use in Criminal Procedural Evidence. *Cand. Diss. Thesis.* Moscow, 2020. 30 p. (In Russian).

11. Jian X., Siegel M., Labudde D., Spranger M. Towards a Joint Semantic Analysis in Mobile Forensics Environments. *Forensic Science International: Digital Investigation*, 2025, V. 52 (3):301846, 1–26. (In English).

12. Tisen O. N. Methodology for Detecting, Recording and Seizing Electronic-Digital Traces in Cases of Crimes Committed Using Cryptocurrencies. *Criminal law*, 2024, no. 3, pp. 69–80. (In Russian).

13. Smushkin A. B. Forensic Aspects for the Dark Net Study for Crimes Investigation Purposes. *Actual problems of Russian Law*, 2022, no. 3(136), pp. 102–111. (In Russian).

14. Meshcheryakov V. A., Tsurluy O. Yu., Kudryavtsev Yu. S. On the Issue of Assessing the Competence of a Forensic Expert. *Discussion Issues of the Theory and Practice of Forensic Science. Materials of the IV International Scientific Conference, Moscow, 25–26 March 2021.* Moscow, Russian State University of Justice, 2021, pp. 417–422. (In Russian).

15. Gavrilin Yu. V. Electronic Memory Devices in Criminal Procedure. Works *of the Academy of Management of the Ministry of Interior of Russia*, 2017, no. 4 (44), pp. 45–50. (In Russian).

16. Rudakov B. V. On the Issue of the Use of Digital (Electronic) Data in Evidence in Criminal Cases. *Legal Order: History, Theory, Practice*, 2021, no. 1 (28), pp. 65–71. (In Russian).

17. Gorbunova E. Yu. Problems of the Quality of Forensic Research (Forensic Computer and Technical Expertise). *Discussion Issues of the Theory and Practice of Forensic Science. Materials of the IV International Scientific Conference, Moscow, 25–26 March 2021.* Moscow, Russian State University of Justice, 2021, pp. 202–207. (In Russian).

Информация об авторе

Харисова Зарина Ирековна *– кандидат технических наук, доцент, доцент кафедры криминалистики Института права*

Information about the Author

Kharisova Zarina Irekovna *– Candidate of Sciences (Engineering), Associate Professor, Chair of Criminalistics, Institute of Law*

Статья поступила в редакцию 30.07.2025; одобрена после рецензирования 18.08.2025; принята к публикации 10.09.2025.
The article was submitted 30.07.2025; approved after reviewing 18.08.2025; accepted for publication 10.09.2025.