**ПРОБЛЕМЫ И ПУТИ СОВЕРШЕНСТВОВАНИЯ ДЕЯТЕЛЬНОСТИ
ПО СОБИРАНИЮ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ
ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ****Зарина Ирековна Харисова**Уфимский юридический институт МВД России, Уфа, Россия,
zarinaid@mail.ru, ORCID: 0000-0002-3902-3459

Аннотация. Необходимость раскрытия органами внутренних дел значительного количества преступлений в сфере компьютерной информации определяет потребность в своевременном и грамотном обнаружении криминалистически значимой компьютерной информации. Проведенное исследование позволило определить основные проблемы, связанные с собиранием цифровых доказательств, а также сформировать направления совершенствования указанной деятельности, заключающиеся в регламентации и алгоритмизации процесса собирания, хранения и использования цифровых данных, имеющих значение для уголовного дела; введении национальных стандартов по их фиксации и анализу; развитии систем сертификации специалистов; расширении перечня используемых программных технико-криминалистических средств; развитии платформ безопасного хранения цифровых доказательств, а также создании нейросетевого криминалистического кластера данных с возможностью оперативного поиска и анализа криминалистически значимой компьютерной информации и формирования на ее основе эффективных методик расследования.

Ключевые слова: расследование преступлений, преступления в сфере компьютерной информации, киберпреступность, цифровые доказательства, цифровая криминалистика, компьютерная криминалистика, сетевая криминалистика, мобильная криминалистика, криминалистика 4.0, технико-криминалистическое средство.

Для цитирования: Харисова З. И. Проблемы и пути совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2025. № 2 (108). С. 116–126.

Original article

**PROBLEMS AND WAYS TO IMPROVE THE COLLECTION
OF DIGITAL EVIDENCE IN CYBERCRIMES INVESTIGATION****Zarina Irekovna Kharisova**Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia,
zarinaid@mail.ru, ORCID: 0000-0002-3902-3459

Abstract. The necessity for law enforcement agencies to solve a significant number of crimes in the field of computer information determines the need for timely and competent detection of forensically significant computer information. The conducted research has identified the main problems associated with the collection of digital evidence and concluded that the primary areas for improving this activity are regulation and algorithmization of the process of collecting, storing, and using digital data relevant to criminal cases; introduction of national standards for their documentation and analysis; development of certification systems for specialists; expansion of the list of software and forensic technical tools used; development of platforms for secure storage of digital evidence; and the creation of a neural network forensic data cluster with the capability for rapid search and analysis of forensically significant computer information and the formulation of effective investigation methodologies based on it.

Keywords: crime investigation, computer crime, cybercrime, digital evidence, digital forensics, computer forensics, network forensics, mobile forensics, forensics 4.0, forensic technology.

For citation: Kharisova Z. I. Problems and ways to improve the collection of digital evidence in cybercrimes investigation // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2025. No. 2 (108). P. 116–126. (In Russ.)

Введение

Развитие индустрии информационных технологий (далее – ИТ), экспоненциальный рост цифровизации большинства социально-экономических процессов, повсеместное использование технических устройств, информационно-телекоммуникационной сети Интернет, а также мобильных средств связи, развитие дистанционного банковского обслуживания, увеличение безналичного денежного оборота и иные факторы, определяющие информатизацию общества, привели к тому, что за прошедшие несколько лет существенно изменились способы, средства и условия совершения преступлений. Указанная тенденция способствовала беспрецедентному росту преступности в сфере компьютерной информации (далее – СКИ), противодействие которой до настоящего времени осложняется несовершенством процесса поиска, фиксации, собирания и оценки криминалистически значимой компьютерной информации, а также отсутствием необходимых технико-криминалистических средств (далее – ТКС).

Важнейшими задачами науки криминалистики из числа специальных являются привлечение данных естественных и технических наук в целях оптимизации научно-технического обеспечения, а также совершенствование криминалистических средств, методов, тактических приемов и методических рекомендаций раскрытия, расследования и предупреждения преступлений. Наиболее важные на сегодняшний день сопутствующие задачи заключаются в синергичной адаптации к современным условиям в плане применения ИТ и разработке новейших технических средств в целях своевременного обнаружения, фиксации и исследования следов (в том числе электронных), образующихся в результате совершения преступных деяний. По этой причине важно рассмотрение типичных проблем и

путей совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в СКИ, что может выступить необходимой правовой основой предупреждения киберпреступности, обеспечения своевременного, законного сбора и использования криминалистически значимой информации в электронной форме.

Методы

В процессе исследования использовалась совокупность общих методов научного познания (описание, обобщение и сравнение), общенаучных (анализ, синтез, системный), частнонаучных (статистический и кибернетический), а также специальных методов (формально-юридический, сравнительно-правовой и научно-технического прогнозирования). Использование указанных приемов позволило провести обобщение и анализ эмпирического материала, а также определить перспективные направления совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в СКИ.

Результаты

Существенное увеличение количества преступлений, связанных с неправомерным доступом к компьютерной информации (статья 272 Уголовного кодекса Российской Федерации (далее – УК РФ)), рост их доли в общем числе преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (далее – ИТТ), низкая раскрываемость указанного вида преступных деяний, а также рост утечек конфиденциальных данных, способный нанести существенный ущерб как отдельным гражданам государства, так и объектам критической информационной инфраструктуры Российской Федерации (статья 274.1 УК РФ), оборонно-промышленного комплекса и смежных отраслей промышленности [1, с. 57], говорит о том, что проводимое

исследование является довольно актуальной задачей. Существенное негативное влияние на обстановку в указанной сфере оказывает сложившаяся международная ситуация, связанная с деятельностью транснациональных организованных преступных групп, нацеленных на хищение персональных данных граждан нашей страны, их неправомерное использование и распространение (статья 272.1 УК РФ). Отдельная проблема заключается в противоправном применении ИТТ организованными преступными группами, которые все чаще используют вредоносное программное обеспечение (далее – ПО) и фишинговые сайты (статья 273 УК РФ). Кроме того, довольно часто нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и инфокоммуникационных сетей приводит к тяжким последствиям или создает угрозу их наступления (статья 274 УК РФ).

В связи с этим необходимо создание надежного барьера противодействия преступлениям именно в СКИ, а также выявление типичных проблем и путей совершенствования деятельности по сборанию цифровых доказательств, которые зачастую являются основными либо единственными свидетельствами преступной деятельности.

Под преступлениями в СКИ понимают законодательно определенные преступные деяния, предусмотренные главой 28 УК РФ [2, с. 6], объединяющей статьи 272, 272.1, 273, 274, 274.1, 274.2. Анализ криминогенной обстановки в Российской Федерации свидетельствует о том, что указанный вид преступности стал одним из ключевых деструктивных факторов общественного развития. Его количественный рост, сопровождающийся качественными изменениями, создает реальную угрозу социально-экономическому развитию, стабильности государственности и национальной безопасности.

Криминализация использования ИТТ усугубляется активным вовлечением в нее организованных преступных групп, которые постоянно ищут новые способы совершения преступлений, используя передовые достижения науки и техники. По этой причине итогом пятилетней работы государств – членов Организации Объединенных Наций стало одобрение разработанной по инициативе Российской Федерации Конвенции против киберпреступности, являющейся первым универсальным договором, предусматривающим укрепление международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием ИТТ¹. Проект резолюции принятого документа подчеркивает особую важность борьбы с указанным видом преступлений, поскольку они зачастую связаны с отмыванием денег, террористическими и экстремистскими актами, неправомерным использованием криптовалют, коррупцией, торговлей людьми, незаконным изготовлением и оборотом оружия, наркотических и психотропных веществ и пр., а статья 23 определяет необходимость принятия на государственном уровне законодательных и иных мер в целях установления полномочий и процедур в отношении уголовных правонарушений, совершенных с помощью ИТТ, акцентируя особое внимание на сборании доказательств в электронной форме.

На сегодняшний день криминалистическая наука оперирует рядом устоявшихся фундаментальных категорий, которые формируют ее основу в виде теоретического аппарата и методологических подходов. К числу основных криминалистических понятий относят такие дефиниции, как доказательство, следственная ситуация, способ совершения и сокрытия преступления, криминалистическое средство, криминалистические прием и рекомендация, тактиче-

¹ Конвенция Организации Объединенных Наций против киберпреступности: укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме А/79/460 от 27 ноября 2024 года // Официальный сайт Организации Объединенных Наций. URL: <https://documents.un.org/doc/undoc/gen/n24/372/06/pdf/n2437206.pdf> (дата обращения: 26.02.2025).

ская комбинация (операция), тактическое решение, криминалистическая характеристика преступного деяния и иные концепты [3, с. 28]. Однако основой предметного поля криминалистики выступает характеристика закономерностей собирания, исследования, оценки и использования доказательств. На основе декомпозиции этих закономерностей наука разрабатывает ТКС, тактические приемы и рекомендации по работе с найденными доказательствами.

Криминалистические методы и средства по источнику происхождения все чаще могут быть результатом междисциплинарного синтеза (в плане использования достижений смежных наук) и по содержанию подразделяются на технические, тактические и методические. Соответственно, надлежащим образом систематизированные совокупности методов расследования и ТКС образуют криминалистическую технику, криминалистическую тактику и криминалистическую методику [4, с. 59].

Материально-вещественные объекты (инструменты, устройства или материалы), функционально предназначенные для обнаружения, фиксации, изъятия и анализа доказательственной информации либо создания препятствий к совершению преступного деяния принято называть ТКС. Условиями применения ТКС и криминалистических приемов являются их допустимость и научная обоснованность, которая означает, что они основаны на положениях той или иной науки, удовлетворяют всем предъявляемым требованиям, а результаты их использования обладают достаточной степенью валидности и достоверности. В первую очередь указанные средства помогают собрать доказательственную базу по уголовному делу, кроме того, именно они применяются для обнаружения, фиксации и изъятия различных следов и иных объектов на месте происшествия, позволяя выявить участников преступления, обеспечивая при этом возможность фиксации обстановки, в которой производится следственное действие [5, с. 6].

Четвертый этап развития криминалистики (криминалистика 4.0) [6, с. 52] свя-

зан с активным внедрением ИТ в жизнедеятельность человека и подразумевает цифровизацию применяемых ТКС в целях раскрытия и расследования преступлений, совершаемых в цифровой среде, что соответствует современным научно-исследовательским приоритетам. Правовые основания применения ТКС представляют собой систему закрепленных норм и принципов, определяющих условия допустимости их задействования и порядок процессуального оформления фактов их использования. Применение ТКС осуществляется в строгом соответствии с Конституцией Российской Федерации, нормами Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) и международного права, т. е. исключительно при наличии правовых оснований для их использования.

Как уже было указано ранее, глобальная информатизация общества затронула не только способы, средства и условия совершения преступлений, но и правила производства следственных действий. Так, в соответствии со статьей 73 УПК РФ важнейшее значение имеют поиск, обнаружение, фиксация и изучение различных следов и вещественных доказательств, позволяющих осуществлять доказывание. Соответственно, под цифровым доказательством, исходя из содержания статьи 74 УПК РФ, понимается любая компьютерная информация, на основе которой суд, прокурор, следователь или дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных имеющих значение обстоятельств.

К основным инструментам, способствующим расследованию преступлений в СКИ, относят средства цифровой криминалистики [7, с. 361], направленные на выявление, извлечение, анализ и сохранение цифровых доказательств, хранящихся на электронных и машинных носителях информации (компьютерная криминалистика), в мобильных средствах связи (мобильная криминалистика), в сетевой среде (сетевая криминалистика), а также в облачных сервисах (облачная

криминалистика) [8, с. 775]. Средствами цифровой криминалистики являются программные и аппаратные средства анализа цифровых доказательств, хранилища электронных данных, устройства их аппаратного восстановления, комплексы перехвата сетевого трафика и т. п.

Основной задачей цифровой криминалистики является развитие и своевременное обновление ТКС в виде ПО [9, с. 181], при этом очевидно, что криминалистическое обеспечение расследования и раскрытия преступлений рассматриваемого вида стратегически целесообразно планировать с возможностью автоматизации рутинных задач, что возможно исключительно с задействованием ИТ, в том числе современных, на базе технологий ИИ, анализа больших данных, хранения доказательств в распределенных системах, т. е. на базе концепции Web 3.0 [10, с. 10].

Таким образом, внедрение ИТ в технико-криминалистическое обеспечение расследования преступлений в СКИ дает возможность формирования значительного массива криминалистически значимой информации, новых криминалистических учетов, их обработки и использования в профессиональной деятельности следователей, дознавателей, оперативных сотрудников, экспертов и специалистов.

Несмотря на наличие правового регулирования, действующая правоприменительная практика в настоящее время довольно часто сталкивается с проблемами поиска, фиксации и исследования цифровых доказательств, их процессуального оформления, достоверности (неизменяемости) и допустимости их в суде, а также рядом технических трудностей, связанных с последующим хранением данных.

Эффективность поиска и собирания криминалистически значимых объектов довольно часто зависит от уровня использования следователем технических средств, ИТТ, а также специальных знаний. Нередки случаи, когда произвести собирание доказательств без использования специальных знаний либо участия в следственном действии

эксперта или специалиста не представляется возможным, что обусловлено, например, применением ультрасовременных технологий при совершении преступлений [11, с. 3]. Так, в отсутствие специальных знаний в области собирания и анализа цифровых доказательств или программных ТКС алгоритм действий следователя может привести к утрате или упущению «виртуальных» следов преступного деяния.

Таким образом, эффективность расследования преступлений в СКИ в большинстве случаев зависит от качества собирания, фиксации и оценки цифровых доказательств путем использования ТКС. Так, например, идентифицировать преступника и определить его причастность к инциденту поможет выявление: IP-адресов и MAC-идентификаторов задействованных устройств; данных лог-файлов, маршрутизаторов и журналов системного ПО [12, с. 142]; метаданных файлов и реестров сетевой активности; фактов использования виртуальных частных сетей и систем прокси-серверов и пр. Восстановить и реконструировать хронологию событий и, как следствие, эффективно спланировать дальнейшие следственные действия позволяет анализ временных меток в информационных системах [13, с. 7], объективность расследования могут обеспечить данные о местоположении мобильного средства связи, анализ коммуникаций участников уголовного процесса, что, в свою очередь, может подтвердить или опровергнуть показания подозреваемых, свидетелей и пр.

К основным проблемам, связанным с поиском цифровых доказательств, можно отнести фрагментарность и изменчивость цифровой информации (создается риск утраты или искажения криминалистически значимой информации, что особенно актуально при работе с оперативной памятью технических средств и облачных сервисов [14, с. 2640]), возможность шифрования и анонимизации данных (значительно затрудняет идентификацию и поиск цифровых доказательств и требует специальных средств противодействия для их обхода), разнообразие среды исследования и невозможность стандарти-

зации процесса выявления доказательств (персональные компьютеры с различными видами операционных систем и носителей информации, мобильные средства связи, облачные хранилища данных, сетевая инфраструктура и прочие устройства, каждое из которых предъявляет свои требования к методам поиска данных). Решение проблем поиска, фиксации и исследования цифровых доказательств при расследовании преступлений в СКИ преимущественно заключается в автоматизации указанных процессов путем использования программных ТКС, поскольку автоматическую классификацию и детектирование киберугроз, в том числе среди больших массивов сведений, в совокупности с геометрически растущим объемом цифровых данных, возможно охватить исключительно используя ПО, в частности, построенного на базе технологий искусственного интеллекта и машинного обучения [15, с. 331].

На сегодняшний день информация, являясь одним из наиболее ценных продуктов для мирового сообщества, часто становится объектом преступного посягательства, при этом ИТ служат орудием такого рода правонарушений. В результате «оцифровки» значительного объема пользовательских данных различными интернет-сервисами и веб-приложениями (сведения о пользовательских устройствах и их индивидуальных настройках, логи авторизации, поведенческие, персональные данные и т. п.) сформировалась возможность использования генерируемой информации в качестве основы для формирования информационно-аналитического кластера распределенных данных с функцией нейросетевого анализа.

Предлагаемый нейросетевой криминалистический кластер на основе общедоступной информации при условии соблюдения установленных нормативными правовыми актами ограничений в отношении распространения такой информации, аналогично криминалистическим учетам в цифровом виде, определил бы возможность гибкой настройки по выдаче отчетов по интересующим следствие направлениям. Необходимость поддержания инфраструктуры пред-

лагаемой системы заключается в плановом и своевременном обновлении сформированных каталогов и инструментов для поиска данных, а также обеспечения соблюдения требований по обработке общедоступных источников, а также грамотного переобучения системы после обновления баз данных. При этом главной проблемой по формированию интеллектуального нейросетевого криминалистического кластера является отсутствие единых стандартов в подходе к охраняемой информации, в частности к персональным данным граждан различных стран. По этой причине актуальной задачей на этапе зарождения проекта являлось бы формирование рассматриваемой информационной системы в рамках реализации для одного государства (национального кластера) либо возможностью создания массива кластеров данных при условии их обезличивания (путем введения условных идентификаторов объектов исследования). Достоинствами формирования нейросетевого криминалистического кластера данных являются повышение эффективности поиска необходимой для раскрытия или расследования информации за счет алгоритмизации этого процесса, удобство обработки значительного количества данных с использованием ключевых слов и фильтров в едином сегменте сети, хранения и использования цифровых доказательств, расширение механизмов оперативного доступа к данным, а также снижение трудозатрат и ресурсов по их поиску.

К проблемам фиксации цифровых доказательств и, как следствие, обеспечения целостности данных и их доказательной силы в суде можно отнести отсутствие единых методологических стандартов по их закреплению, недостаток сертифицированных программных ТКС, а также значительные временные и трудовые издержки неавтоматизированной фиксации криминалистически значимой информации. Непосредственное исследование данных осложняется их разнородностью, величиной массивов информации, подлежащих обработке. Это требует использования специализированного ПО и высокопроизводительных вы-

числительных мощностей, что в совокупности обуславливает увеличение времени, затрачиваемого на анализ. По этой причине целесообразна разработка и активное использование адаптивных программных ТКС, позволяющих в условиях постоянной трансформации и эволюции киберпреступности систематизировать (кодифицировать) преступления в СКИ, в автоматизированном виде обеспечить как поиск, так и фиксацию доказательств в цифровой среде различного генеза.

Достоверность (неизменяемость) и допустимость изъятых цифровых доказательств может обеспечить расчет контрольных сумм файлов. Как известно, основным способом установления дублирования, равно как определения идентичности двух электронных файлов, является дедупликация (тестовая проверка данных, заключающаяся в расчете их контрольных сумм (хеш-функций)) [16, с. 44]. По результатам выполнения теста в виде хеширования и установления полного соответствия хеш-функций можно сделать вывод об идентичности сравниваемых файлов. Соответственно, рассчитанная контрольная сумма электронного файла исключает проблему установления достоверности (неизменяемости) цифровых доказательств в процессе ее копирования или исследования. По этой причине необходимо рассмотреть возможности учета контрольных сумм цифровых доказательств в целях последующей допустимости их в суде, либо альтернативной возможности в виде внедрения блокчейн-платформ на базе распределенных реестров для обеспечения неизменности выявляемых данных [17, с. 4380].

Достоверность доказательств в первую очередь оценивается с точки зрения уголовно-процессуального законодательства или иного законодательства, относящегося к уголовному судопроизводству, но стоит отметить, что источник получения доказательств должен быть своевременно проверен, должно быть подтверждение существования источника и факт получения доказательства. Относимость доказательств раскрывается применительно ко всем видам

доказательств, так как доказательства, которые были получены в ходе проведения следственных действий, должны действительно иметь место и связь с подозреваемым или обвиняемым или же с фактом совершенного преступления.

Помимо исследования, все доказательства нуждаются в оценке. Это также род мыслительной деятельности субъектов расследования, при которой доказательства должны «придерживаться» критериев достоверности, относимости и допустимости. Это нужно для того, чтобы при рассмотрении уголовного дела судом не возникло замечаний, отводов и ходатайств со стороны защиты. Стоит отметить, что все цифровые доказательства должны исследоваться и оцениваться в совокупности, так как отдельно взятое доказательство может противоречить другому, отдельно рассматриваемому, доказательству в деле.

К насущным проблемам процессуального оформления цифровых доказательств можно отнести неопределенность процессуального статуса цифровых данных. Так, в соответствии со статьей 84.1 УПК РФ электронные носители информации признаются вещественными доказательствами, однако критерии их допустимости не раскрываются. Кроме того, отсутствует четкая регламентация процедуры изъятия таких данных, например, с облачных сервисов и прочих хранилищ. Имеются пробелы и в соблюдении правил изъятия и фиксации цифровых доказательств при удаленном доступе к данным, когда в соответствии со статьей 177 УПК РФ для этого требуется участие понятых. Это может привести к оспариванию доказательств в суде. Существенной проблемой является поиск и дальнейшее приобщение к делу криминалистически значимой информации, полученной из открытых источников сети Интернет и сервисов OSINT-разведки [18, с. 52], деятельность которых признается незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну, что стало особенно важно в свете дополнения УК РФ статьей 272.1, устанавливающей

уголовную ответственность за незаконные сбор и хранение персональных данных, а также создание на их основе информационных ресурсов, предназначенных для распространения личной информации. Указанная коллизия может породить прецеденты, когда полученные цифровые доказательства признаются недопустимыми. С целью устранения данной проблемы возможно развитие систем сертификации специалистов, задействованных в расследовании и раскрытии преступлений в СКИ.

Решение проблемы процессуального оформления цифровых доказательств при расследовании преступлений в СКИ требует комплексного подхода, включающего не только юридические нормы, но и технические меры, а также усовершенствованные криминалистические методики. В целях соблюдения принципа целостности и аутентичности цифровых доказательств целесообразно придерживаться широко распространенного в настоящее время принципа «цепочек поставок» (chain of custody) [19, с. 12], который сможет обеспечить фиксацию всех этапов работы с доказательством. Проблема обеспечения сохранности цифровых доказательств при расследовании преступлений в СКИ, безусловно, требует технологических инноваций. Так, предотвратить утрату данных можно путем организации центров обработки данных на основе распределенных баз, облачных или RAID-массивов с возможностью расчета контрольных сумм и контроля версий хранилищ либо внедрения блокчейн-технологий с временными метками, что обеспечит неизменность данных и прозрачность процесса их хранения. При этом защиту цифровых доказательств от посягательств можно обеспечить использованием квантово-устойчивых алгоритмов шифрования [20, с. 12], что является одним из перспективных направлений реализации подобных систем в будущем.

Заключение

Актуальность совершенствования механизма собирания цифровых доказательств в Российской Федерации обусловлена ростом преступности в СКИ, обновлением способов,

средств и условий совершения преступлений, а также технологическими вызовами. Реализация выдвигаемых предложений позволит повысить эффективность раскрытия и расследования указанного вида преступных деяний, обеспечить юридическую и техническую состоятельность цифровых доказательств, а также усилить взаимодействие между государственными органами и частным сектором в борьбе с киберугрозами.

Проведенное исследование позволило определить основные проблемы в деятельности по собиранию цифровых доказательств, заключающиеся в отсутствии средств автоматизации поиска, фиксации и исследования цифровых доказательств, четких регламентов их процессуального оформления, инструкций по обеспечению достоверности (неизменяемости) и их допустимости, а также хранению данных.

В качестве возможного решения указанных проблем предложена система в виде хранилища криминалистически значимой компьютерной информации с функцией нейросетевого анализа данных (нейросетевой криминалистический кластер). Описанное в работе решение может использоваться в целях повышения эффективности поиска необходимых для раскрытия и расследования преступлений в СКИ сведений, удобства обработки значительного количества данных с использованием ключевых слов и фильтров в едином сегменте сети, снижения трудозатрат и ресурсов поиска криминалистически значимой информации сотрудниками органов внутренних дел.

Проведенное исследование позволяет сделать вывод, что основными направлениями совершенствования деятельности по собиранию цифровых доказательств при расследовании преступлений в СКИ являются:

– подробная регламентация и алгоритмизация процесса собирания, хранения и использования цифровых доказательств, что в условиях постоянной трансформации и эволюции киберпреступности возможно, например, при тщательной классификации способов, средств и условий совершаемых преступлений, а также их универсальной

кодификации в целях разработки общей концепции их расследования и выработки соответствующих заданным условиям алгоритмов расследования;

– введение национальных стандартов по фиксации и анализу цифровых доказательств, а также развитие систем сертификации специалистов, задействованных в расследовании и раскрытии преступлений в СКИ;

– расширение перечня программных ТКС для автоматизированного поиска, фиксации и исследования цифровых доказательств, на базе технологий искусствен-

ного интеллекта и анализа больших данных;

– развитие облачных платформ для безопасного и неизменного хранения цифровых доказательств с применением блокчейн-технологий и распределенных реестров;

– создание единого нейросетевого криминалистического кластера данных с возможностью оперативного доступа к цифровым доказательствам, поиска и обработки криминалистически значимой информации с использованием ключевых слов и фильтров в едином сегменте сети.

СПИСОК ИСТОЧНИКОВ

1. Комплексный анализ состояния преступности в Российской Федерации и ожидаемые тенденции ее развития: аналитический обзор / М. В. Гончарова, М. М. Бабаев, Р. В. Черкасов и др. Москва: ФГКУ «ВНИИ МВД России», 2024. 87 с.

2. Попов А. Н. Преступления в сфере компьютерной информации. Санкт-Петербург: Санкт-Петербургский юридический институт Университета прокуратуры Российской Федерации, 2018. 68 с.

3. Эксархопуло А. А., Макаренко И. А., Зайнуллин Р. И. Криминалистика. Теоретический курс: монография. Уфа: НИИ ППГ, 2022. 650 с.

4. Аверьянова Т. В. Криминалистика. М.: Норма, 2023. 928 с.

5. Козлов А. Е., Макарова Е. Н., Романова О. Л. Современные технико-криминалистические средства, применяемые в ходе осмотра места происшествия. Санкт-Петербург: СПбУ МВД России, 2024. 64 с.

6. Нестеров А. В. Виртуальные следы в криминалистике. М.: Издательство КноРус, 2024. 154 с.

7. Nelufule N. Intersection of electronic security and digital forensics: data protecting techniques and uncovering data clues // Towards new e-infrastructure and e-services for developing countries. 2025. No. 587. P. 351–367.

8. Tiwari N., Baroniya Y., Bharadwaj V. Cyber and digital forensic // Textbook of forensic science. 2023. No. 25. P.773–803.

9. Garrie D. B., Gordon L. M., Newman B. Digital forensic investigations and ediscovery // Uncovering Digital Evidence. 2024. No. 1. P. 155–191.

10. Adams T. A. Trends, challenges and opportunities of engaging digital forensics for cybercrime investigations // Advances in multidisciplinary and scientific research journal publication. 2024. No. 15 (1). P. 1–12.

11. Thakur K. S., Ahuja R. Safeguarding justice employing blockchain-enabled secure chain of custody framework for digital evidence // Innovations in electrical and electronic engineering. 2024. No. 115. P. 1–11.

12. Федотов Н. Н. Форензика – компьютерная криминалистика. М.: Юридический мир, 2007. 432 с.

13. Cantelli-Forti A., Longo G., Lupia F. A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence. International journal of information security. 2025. No. 24 (81). P. 1–14.

14. Yi X., Zhou Y., Lin Y. et al. Digital rights management scheme based on redactable blockchain and perceptual hash. Peer-to-peer networking and applications. 2023. No.16. P. 2630–2648.

15. Kreso I. Using blockchain technology for preserving digital evidence in digital forensics // Knowledge international journal. 2025. No. 68 (3). P. 331–336.

16. Medjedovic Dz., Tahirovic E. Algorithms and data structures for massive datasets. New York: Manning Shelter Island, 2024. 340 p.

17. Ryu J. H., Sharma P. K., Jo J. H. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The journal of supercomputing*. 2019. No. 75. P. 4372–4387.
18. Омельченко В. А., Фаниев П. А. Использование программного обеспечения категории Open Source, для создания анонимной рабочей среды и проведения разведки OSINT. М.: Издательство «Перо», 2024. 69 с.
19. Nath S., Summers K., Jaejong B. Digital evidence chain of custody: navigating new realities of digital forensics // *Intelligent systems, and applications*. 2024. No. 6. P. 11–20.
20. Xiong J., Shen L., Liu Y. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption // *Scientific Reports*. 2025. No. 15 (3). P. 1–15.

REFERENCES

1. Comprehensive analysis of the state of crime in the Russian Federation and expected trends in its development: an analytical review M. V. Goncharova, M. M. Babaev, R. V. Cherkasov et al. Moscow: All-Russian Research Institute, 2024. 87 p. (In Russ.)
2. Popov A. N. Crimes in the field of computer information. Saint Petersburg: Saint Petersburg Law Institute of the University of the Prosecutor's Office of the Russian Federation, 2018. 68 p. (In Russ.)
3. Eksarkhopulo A.A., Makarenko I.A., Zainullin R.I., Forensic Science. Theoretical Course: monograph. Ufa: Research Institute of PPG, 2022. 650 p. (In Russ.)
4. Averianova T. V. Forensic Science. Moscow: Norma, 2023. 928 p. (In Russ.)
5. Kozlov A. E., Makarova E. N., Romanova O. L. Modern technical and forensic tools used during crime scene inspection. Saint Petersburg: Saint Petersburg University of the Ministry of Internal Affairs of Russia, 2024. 64 p. (In Russ.)
6. Nesterov A.V. Virtual traces in forensic science. Moscow: Knorus Publishing House, 2024. 154 p. (In Russ.)
7. Nelufule N. Intersection of electronic security and digital forensics: data protecting techniques and uncovering data clues // *Towards new e-infrastructure and e-services for developing countries*. 2025. No. 587. P. 351–367.
8. Tiwari N., Baroniya Y., Bharadwaj V. Cyber and digital forensic // *Textbook of forensic science*. 2023. No. 25. P. 773–803. (In Eng.)
9. Garrie D. B., Gordon L. M., Newman B. Digital forensic investigations and ediscovery // *Uncovering Digital Evidence*. 2024. No. 1. P. 155–191. (In Eng.)
10. Adams T. A. Trends, challenges and opportunities of engaging digital forensics for cybercrime investigations // *Advances in multidisciplinary and scientific research journal publication*. 2024. No. 15 (1). P. 1–12. (In Eng.)
11. Thakur K. S., Ahuja R. Safeguarding justice employing blockchain-enabled secure chain of custody framework for digital evidence // *Innovations in electrical and electronic engineering*. 2024. No. 115. P. 1–11. (In Eng.)
12. Fedotov N. N. Forensics – computer forensics. Moscow: Legal World, 2007. 432 p. (In Russ.)
13. Cantelli-Forti A., Longo G., Lupia F. A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence. *International journal of information security*. 2025. No. 24 (81). P. 1–14. (In Eng.)
14. Yi X., Zhou Y., Lin Y. et al. Digital rights management scheme based on redactable blockchain and perceptual hash. *Peer-to-peer networking and applications*. 2023. No. 16. P. 2630–2648. (In Eng.)
15. Kreso I. Using blockchain technology for preserving digital evidence in digital forensics // *Knowledge international journal*. 2025. No. 68 (3). P. 331–336. (In Eng.)
16. Medjedovic Dz., Tahirovic E. Algorithms and data structures for massive datasets. New York: Manning Shelter Island, 2024. 340 p. (In Eng.)
17. Ryu J. H., Sharma P. K., Jo J. H. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The journal of supercomputing*. 2019. № 75. P. 4372–4387. (In Eng.)
18. Omelchenko V. A., Faniev P. A. Using open-source software to create an anonymous working environment and conduct OSINT intelligence. Moscow: Pero Publishing House, 2024. 69 p. (In Russ.)
19. Nath S., Summers K., Jaejong B. Digital evidence chain of custody: navigating new realities of digital forensics // *Intelligent systems, and applications*. 2024. № 6. P. 11–20. (In Eng.)

20. Xiong J., Shen L., Liu Y. Enhancing IoT security in smart grids with quantum-resistant hybrid encryption // Scientific Reports. 2025. № 15 (3). P. 1–15. (In Eng.).

Информация об авторе:

З. И. Харисова, кандидат технических наук, доцент.

Information about the author:

Z. I. Kharisova, Candidate of Technology, Associate Professor.

Статья поступила в редакцию 09.03.2025; одобрена после рецензирования 21.04.2025; принята к публикации 20.06.2025.

The article was submitted 09.03.2025; approved after reviewing 21.04.2025; accepted for publication 20.06.2025.