

Карабинцева И.К.

Волгоградская академия МВД России

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Для изучения современных методов криминалистического исследования цифровой информации следует дать определение термину «цифровой след». Д.В. Бахтеев утверждает, что цифровую информацию нельзя полностью отнести ни к материальным, ни к идеальным следам¹. Он объясняет это двойственным характером цифровых данных. С одной стороны, цифровые следы нельзя отнести к идеальным, поскольку они сохраняют объективные признаки взаимодействия преступника с цифровой средой. С другой стороны, такие следы также не относятся к материалу в чистом виде, так как зачастую их существование ограничено виртуальной формой – например, в формате программного кода или информационного пакета. Е.Р. Россинская считает, что цифровые следы имеют материальную природу, так как всегда фиксируются на физических носителях, таких как оперативная память, жесткие диски, серверы и другие устройства². По мнению Э.Р. Бураканова «цифровой след – это информация на электронных носителях, которая получена через электромагнитные взаимодействия или передана по каналам связи с помощью электромагнитных сигналов»³.

Современное развитие криминалистической науки и цифровых технологий приводит специалистов к мнению о необходимости выделения цифровых следов в самостоятельную категорию. Это обусловлено их уникальными характеристиками, сложностью идентификации и невозможностью однозначного включения в существующую классификацию следов⁴.

Цифровая информация по своим характеристикам обладает определенными сходствами с вещественными доказательствами,

например вредоносное программное обеспечение, и документальными источниками, такими как сообщения в социальных сетях или данные, размещенные на веб-сайтах. При этом цифровые доказательства имеют уникальные особенности, которые заключаются в отсутствии привязанности такой информации к физическим лицам, поскольку создание, хранение и обработка цифровых данных осуществляются с использованием электронно-вычислительных средств. Кроме того, цифровая информация недоступна для непосредственного восприятия человеком без привлечения специализированных технических инструментов.

С данной позицией согласуются выводы А.В. Шигурова и Е.И. Шигуровой, утверждающих, что уголовно-процессуальное законодательство должно содержать специальный правовой механизм, регламентирующий взаимодействие с электронными носителями информации. Такой механизм должен учитывать особенности не только самих источников данных, но и характер содержащихся в них электронных следов, а также методы их обнаружения, фиксации и исследования⁵.

Для получения цифровой информации в рамках уголовного дела существует несколько процессуальных способов.

1. Обыск традиционно является главным способом для сбора доказательств, применяемым в ходе расследования уголовного дела. В рамках данного действия следователь вправе изымать компьютерное оборудование и носители информации, а также проводить осмотр помещений или объектов, предположительно связанных с хранением цифровой информации.

¹ Бахтеев Д.В. Криминалистическая классификация цифровой доказательственной информации // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) : сборник статей международной научно-практической конференции. М.: Академия управления МВД России, 2018. С. 44-49.

² Россинская Е.Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации // Юридический вестник Самарского университета. 2019. № 4. С. 144-151.

³ Бураканова Э.Р. Цифровые следы в криминалистике // Тенденции развития науки и образования. 2023. № 93-4. С. 66-68.

⁴ Денисов И.М., Лещинский М.И. Криминалистическое исследование цифровой информации // Международный журнал гуманитарных и естественных наук. 2023. № 1-1 (76). С. 139-141.

⁵ Шигуров А.В., Шигурова Е.И. Проблемы правовой регламентации использования электронных следов и электронных носителей информации при производстве по уголовному делу // Гуманитарные и политико-правовые исследования. 2020. № 1 (8). С. 53-63.

2. Изъятие представляет собой дополнительный способ получения компьютерной информации, который применяется в случае невозможности извлечения данных традиционными методами. При изъятии следователь изымает электронные устройства или носители данных, после чего они направляются на экспертизу. Судебные эксперты проводят анализ изъятых материалов для установления их ценности как доказательств.

3. Компьютерно-техническая экспертиза является одним из важнейших инструментов для изучения цифровых следов. По своей сущности это судебная экспертиза, направленная на содействие следователю или суду в установлении фактических обстоятельств посредством анализа данных, находящихся на электронных носителях¹. Примеры расследуемых преступлений включают в себя кибератаки, нарушения авторских прав, утечки конфиденциальных данных, хищение информации и хакерские атаки.

Эффективное противодействие преступлениям, совершаемым с применением компьютерных технологий, возможно только при тесной координации усилий следователя и специалиста, обладающего специализированными знаниями в данной сфере. Указанное взаимодействие может осуществляться посредством привлечения специалистов Экспертно-криминалистических центров МВД. Формы их совместной работы охватывают несколько направлений: консультационную поддержку, участие специалиста в следственных действиях, а также проведение экспертных исследований.

Необходимость привлечения специалиста при участии в производстве следственных действий обусловлена наличием у него специальных познаний. Так, при производстве допроса целесообразно привлечь специалиста, поскольку следователь, не обладающий достаточными знаниями в области цифровых технологий или компьютерной терминологии, может испытывать затруднения при квалификации действий подозреваемого или выявления значимых деталей, что ставит под угрозу раскрытие преступления. В этом случае компетентный специалист привлекается как на этапе подготовки допроса (разработки тактики, формулирования технически грамотных вопросов), так и к

непосредственному участию в допросе. В процессе взаимодействия специалист разъясняет сложные термины, помогает уточнять информацию и оказывает содействие в фиксации тех данных, которые могут быть необходимы для дальнейшего расследования.

В заключение следует отметить, что процесс цифровизации общества ставит перед криминалистической наукой новые задачи, требующие комплексного подхода.

Среди способов совершенствования нормативно-правового регулирования в сфере исследования цифровой информации в криминалистике выделяют следующее.

1. В настоящее время понятийный аппарат, связанный с исследованием следов преступной деятельности, демонстрирует недостаточную степень разработанности в условиях цифровизации. Поэтому существует необходимость выделения в рамках криминалистического учения самостоятельной категории цифровых следов, и разработать дефиницию понятия «цифровой след», что позволит структурировать знания о данном объекте и определить характерные признаки, формы и сущность цифровой информации.

2. Эффективность расследования преступлений, связанных с информационными технологиями, во многом зависит от профессиональной подготовки участников уголовного процесса и их способности взаимодействовать в условиях высокого уровня технической сложности. Особое значение приобретает сотрудничество следователя и специалиста, обладающего специальными познаниями в сфере компьютерных технологий. Это взаимодействие должно стать неотъемлемой частью процессуального обеспечения расследования, особенно при обнаружении и анализе цифровых следов, которые обладают значительной спецификой по сравнению с традиционными материальными следами.

3. Дополнительно следует расширить специальный кадровый резерв криминалистов с узкой профессиональной специализацией в области IT-технологий. Устранение данного квалификационного пробела представляется важной задачей для повышения уровня эффективности расследования преступлений в условиях цифровой трансформации общества.

¹ Трошенкова А.И. Роль судебной компьютерно-технической экспертизы в раскрытии преступлений // Международный журнал гуманитарных и естественных наук. 2020. № 12-2 (51). С. 91-94.