УДК 343.13

Дмитриева А.А.
магистрант
кафедра уголовного процесса,
криминалистики и основ судебной экспертизы
Красноярский государственный аграрный университет
(г. Красноярск, Россия)

ЦИФРОВЫЕ СЛЕДЫ И ПРОБЛЕМЫ ДОКАЗЫВАНИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ ЗАКУПОК

Аннотация: *в статье исследуются особенности обнаружения, фиксации и использования цифровых следов при расследовании преступлений в сфере государственных и муниципальных закупок. Рассматриваются типичные следственные ситуации, связанные с распределением информации между электронными площадками, корпоративной перепиской, мессенджерами и облачными хранилищами. Анализируются вопросы установления источника цифровых данных, идентификации пользователя, сохранения целостности и процессуального закрепления информации. Обосновывается необходимость сочетания специальных криминалистических процедур с процессуальными гарантиями и проверкой цифровых сведений в совокупности с другими доказательствами.*

Ключевые слова: *цифровой след, цифровое доказательство, государственная закупка, электронная переписка, облачное хранилище, уголовное судопроизводство, допустимость доказательств, криминалистическая фиксация.*

Переход закупочной деятельности в электронную форму существенно изменил источники информации, имеющие значение для расследования преступлений. Данные о подготовке закупки, действиях комиссии, подаче заявок, заключении и исполнении контракта могут находиться одновременно в Единой информационной системе, на электронных торговых площадках, в корпоративной почте, мессенджерах, облачных хранилищах, бухгалтерских

программах и системах дистанционного банковского обслуживания. Поэтому установление механизма преступления требует не только изучения содержания отдельных документов, но и реконструкции истории их создания, изменения, передачи и использования.

Уголовно-процессуальное законодательство не закрепляет цифровую информацию в качестве самостоятельного вида доказательств, однако сведения в электронной форме могут использоваться в рамках системы, предусмотренной ст. 74 УПК РФ, и оформляться в предусмотренных законом процессуальных источниках. Электронные документы и иные носители информации могут приобретать значение иных документов либо вещественных доказательств с учетом характера содержащихся в них сведений и условий их получения. Следовательно, цифровая форма сама по себе не определяет доказательственный статус информации: имеют значение источник, способ обнаружения, законность получения, фиксация и возможность проверки.

Рассмотрим несколько возможных следственных ситуаций. Первая следственная ситуация характеризуется наличием цифровых следов в открытом или относительно доступном состоянии. В материалах закупки могут сохраняться извещения, документация, протоколы рассмотрения заявок, сведения о победителе, контракты, документы об исполнении и данные об электронной подписи. В такой ситуации первоначальная задача состоит не только в получении содержимого файлов, но и в установлении истории их формирования: времени размещения, последующих изменений, пользователя, совершившего соответствующие действия, и связи этих действий с конкретной процедурой закупки.

Вторая ситуация возникает, когда цифровые следы распределены между несколькими информационными ресурсами. Например, сведения о закупке находятся в ЕИС, переписка должностных лиц – в корпоративной почте или мессенджере, проекты технического задания – в облачном хранилище, а данные о фактическом исполнении контракта – в бухгалтерской и складской системах. Доказательственное значение в таком случае имеет не отдельный файл, а

совокупность взаимосвязанных данных. Указание в переписке на изменение технического задания должно сопоставляться с версиями документа, журналами доступа, временем публикации закупки, электронной подписью и последующими платежами [1, 4].

Третья ситуация связана с угрозой утраты или изменения цифровой информации. Сообщения могут удаляться автоматически, файлы – перемещаться или удаляться из облака, журналы событий – перезаписываться, а доступ к почтовому ящику или учетной записи – прекращаться. Цифровые сведения следует рассматривать как нестабильный объект доказывания, требующий своевременной фиксации. Промедление способно привести к утрате истории изменений, резервных копий и данных, позволяющих установить пользователя и последовательность действий [6].

Четвертая ситуация возникает при использовании шифрования, анонимных учетных записей, VPN-сервисов и технических средств сокрытия личности пользователя. В этих случаях необходимо разграничивать принадлежность учетной записи, фактический доступ к ней и совершение конкретного действия определенным лицом. Наличие аккаунта, телефонного номера или IP-адреса не всегда позволяет достоверно идентифицировать пользователя. Для такого вывода требуется сопоставление данных об устройствах, времени входа, сетевых соединениях, содержании переписки, сведениях о местонахождении лица и результатах осмотра техники.

Пятая ситуация обусловлена хранением информации у третьих лиц или на удаленных серверах. Данные могут находиться у оператора связи, владельца электронной площадки, администратора корпоративной системы или провайдера облачного сервиса. Изъятие компьютера или смартфона не гарантирует получения полной истории операций, поскольку устройство нередко является только точкой доступа к информации, физически размещенной на удаленном сервере. Поэтому в план расследования необходимо включать своевременное направление законных запросов о сохранении и предоставлении

конкретных данных, а также получение сведений о действиях пользователей и истории версий файлов [4].

При осмотре переписки в мессенджерах и электронной почте важно сохранять не только отдельные сообщения, но и их контекст. В протоколе целесообразно указывать идентификаторы аккаунтов, сведения о группах и каналах, доступные регистрационные данные, даты и время сообщений, сведения о вложениях, отредактированных или удаленных сообщениях, последовательность диалога и данные об устройстве, с которого осуществлялся доступ. Скриншот может выступать наглядным способом фиксации, однако не должен подменять получение исходных данных: отдельное изображение экрана не всегда позволяет проверить отправителя, время создания, факт изменения и целостность информации [1].

При исследовании облачных хранилищ необходимо устанавливать не только наличие файла, но и историю его создания, изменения, перемещения, удаления и восстановления. Значимыми объектами являются журналы доступа, перечень пользователей, история версий, сведения о синхронизации, ссылки общего доступа и данные о скачивании файла. При наличии технической возможности целесообразно получать сведения непосредственно от оператора сервиса, поскольку локальная копия может не содержать полной истории операций. Аналогичный подход применяется к журналам событий информационных систем: следует установить, какое действие было зарегистрировано, в какой момент, из-под какой учетной записи и с использованием какого технического средства.

Криминалистическая достоверность цифровой информации зависит от сохранения исходного состояния и возможности воспроизвести действия по ее получению. При работе с электронными носителями необходимо учитывать положения ст. 164.1 УПК РФ и правила соответствующего следственного действия. При наличии технической возможности создается криминалистическая копия, исключающая непосредственное исследование исходного носителя. В протоколе фиксируются вид и характеристики носителя,

состояние устройства, примененные программные средства, дата и время копирования, способ получения копии и лица, осуществлявшие доступ к информации.

Для контроля неизменности данных могут рассчитываться контрольные хеш-значения. Совпадение таких значений подтверждает неизменность сравниваемых наборов данных после расчета, но не доказывает истинность их содержания и не устанавливает автора файла. Подложный документ также может быть корректно скопирован и хеширован. Поэтому хеширование является технической гарантией целостности, но не самостоятельным доказательством подлинности. Необходимо документировать всю цепочку хранения: обнаружение, копирование, передачу, исследование и хранение цифрового объекта, указывая время, способ и ответственных лиц [10].

Проверка электронной подписи является важным, но не исчерпывающим элементом исследования электронного документа. Необходимо установить вид подписи, статус сертификата в момент подписания, целостность документа и полномочия лица, использовавшего ключ. Вместе с тем связь документа с сертификатом и фактическое совершение действия конкретным человеком – взаимосвязанные, но не тождественные обстоятельства. Поэтому сведения о подписи должны сопоставляться с журналами авторизации, данными об устройстве, графиком работы, перепиской, свидетельскими показаниями и обстоятельствами хранения ключевого носителя [9].

К числу наиболее существенных проблем относятся недостаток специалистов, технологическая сложность отдельных платформ, неполнота журналов событий, распределенное хранение данных и противодействие заинтересованных лиц. Дополнительный риск возникает при необоснованном изъятии техники без участия специалиста: такие действия могут изменить системные данные, затруднить деятельность организации и создать основания для сомнений в допустимости полученной информации. Не менее важно учитывать законность доступа к информации. Публичность сведений о закупке

не означает открытость личной переписки, персональных данных, банковских операций и охраняемой законом тайны.

Представляется целесообразным разработать единые ведомственные и межведомственные стандарты первичного реагирования на цифровой инцидент, изоляции устройств, создания криминалистических копий, проверки их целостности, документирования действий специалиста и передачи объектов на экспертизу. Такие стандарты должны быть совместимы с процедурами операторов электронных площадок, государственных информационных систем, банков и облачных сервисов. Перспективным является развитие механизмов оперативного сохранения конкретных данных до получения необходимых процессуальных разрешений при условии соблюдения установленных законом гарантий.

Заслуживает внимания предложение о закреплении более подробных требований к сохранению истории версий документов, журналов действий пользователей и сведений об электронной подписи в информационных системах закупок. Электронный документ целесообразно рассматривать не изолированно, а как результат последовательности действий пользователя и системы. Фиксация идентификатора пользователя, даты и времени действия, сведений об устройстве, сетевом адресе и истории версий повышает проверяемость цифровых объектов и позволяет точнее восстанавливать механизм закупочной процедуры. Одновременно необходимо обеспечить защиту персональных данных, коммерческой и иной охраняемой законом тайны.

Таким образом, цифровые следы приобретают особое значение при расследовании преступлений в сфере закупок, поскольку отражают не только содержание электронных документов, но и историю действий участников в информационной среде. Эффективность доказывания зависит от своевременного обнаружения данных, законности доступа, правильной фиксации, установления источника происхождения, проверки целостности и идентификации фактического пользователя. Ни скриншот, ни IP-адрес, ни хеш-значение, ни электронная подпись по отдельности не позволяют сделать окончательный

вывод о виновности лица. Цифровая информация должна оцениваться в совокупности с документальными, финансовыми, материальными и свидетельскими сведениями.

СПИСОК ЛИТЕРАТУРЫ:

1. Гамбарова Е.А. Изъятие цифровых следов из сети Интернет и использование их в доказывании: уголовно-процессуальные аспекты // Вектор науки Тольяттинского государственного университета. Серия «Юридические науки». 2023. № 3 (54). С. 13–19 https://doi.org/10.18323/2220-7457-2023-3-13-19
2. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... д-ра юрид. наук: 12.00.09. Воронеж, 2001. 39 с.
3. Мещеряков В.А. Теоретические основы механизма следообразования в цифровой криминалистике: монография. М.: Проспект, 2022. 176 с.
4. Петрова О.А. Проблемы изъятия электронных носителей информации в отечественном уголовном процессе // Юридический вестник Кубанского государственного университета. 2021. № 1 (13). С. 62–71
5. Россинская Е.Р. Современные проблемы судебной экспертизы в условиях цифровизации и пути их разрешения // Актуальные проблемы российского права. 2021. № 9 (178). С. 60–64
6. Сидорова Е.З. Цифровые доказательства в уголовном процессе: проблемы теории и практики // Вестник Московского университета МВД России. 2022. № 3. С. 178–179
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921
8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165
9. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Российская газета. 08.04.2011. № 75
10. Шрамко А.В. Цифровые доказательства в уголовном судопроизводстве: проблемы допустимости и достоверности // Законность. 2021. № 11. С. 42–47

Dmitrieva A.A.
master's degree student
Department of Criminal Procedure, Criminalistics
and Fundamentals of Forensic Examination
Krasnoyarsk State Agrarian University
(Krasnoyarsk, Russia)

DIGITAL TRACES AND EVIDENTIARY CHALLENGES IN INVESTIGATIONS OF CRIMES INVOLVING STATE AND MUNICIPAL PROCUREMENT

Abstract: *the article examines the detection, documentation, and use of digital traces in investigations of crimes involving state and municipal procurement. It considers typical investigative situations in which information is distributed across electronic procurement platforms, corporate correspondence, messaging apps, and cloud storage services. The article analyzes issues related to identifying digital data sources and users, preserving data integrity, and documenting information in accordance with criminal procedure. It argues that specialized forensic procedures must be combined with procedural safeguards and that digital information must be assessed alongside other evidence.*

Keywords: *digital trace, digital evidence, state procurement, electronic correspondence, cloud storage, criminal proceedings, admissibility of evidence, forensic documentation.*