УДК 4414

Зиннятуллин Марат Ренатович,
аспирант 1 года обучения
юридического факультета
Ульяновского государственного университета
РФ, г. Ульяновск

РАЗВИТИЕ СУДЕБНОЙ И СЛЕДСТВЕННОЙ ПРАКТИКИ РАБОТЫ С ЦИФРОВЫМИ ДОКАЗАТЕЛЬСТВАМИ В РОССИЙСКОЙ ФЕДЕРАЦИИ В ПЕРИОД 1990 – 2020 ГОДОВ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ВЫПОЛНЕНИЯ ПРИНЦИПОВ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация: *В статье исследуется эволюция института цифровых доказательств в российском уголовном процессе с 1990-х годов по настоящее время. Выделяются три ключевых этапа развития: первый — период правового вакуума, когда правоприменителям приходилось адаптировать устаревшие нормы УПК РСФСР к новым реалиям; второй — этап становления практики, когда Верховным Судом были даны первые ориентиры, а ключевую роль стала играть компьютерно-техническая экспертиза; третий — переломный момент законодательной формализации с принятием статьи 81.1 УПК РФ, разделившей материальный носитель и информацию на нем.*

Ключевые слова: *Цифровые доказательства, УПК РФ, судопроизводство.*

Annotation: *The article explores the evolution of the institution of digital evidence in the Russian criminal process from the 1990s to the present day. It identifies three key stages of development: the first stage was a period of legal vacuum, where law enforcement agencies had to adapt the outdated norms of the*

RSFSR Criminal Procedure Code to the new realities; the second stage was the formation of practice, where the Supreme Court provided the first guidelines and computer-technical expertise began to play a crucial role; and the third stage was a turning point in legislative formalization with the adoption of Article 81.1 of the Criminal Procedure Code of the Russian Federation, which separated the material medium and the information on it.

Key words: *Digital evidence. Criminal Procedure Code of the Russian Federation. Legal proceedings.*

Развитие практики использования цифровых доказательств в российском уголовном судопроизводстве представляет собой наглядный пример того, как правовая система пыталась догнать технологическую революцию. Этот тридцатилетний путь можно разделить на три ключевых этапа, каждый из которых характеризовался своими вызовами и способами их преодоления через судебные решения и следственные методики.

Первый этап (1990-е – начало 2000-х): период правового вакуума и судебной импровизации. В эпоху, когда персональные компьютеры и мобильная связь только начинали входить в жизнь, Уголовно-процессуальный кодекс РСФСР 1960 года оставался нем перед цифровым миром. Законодатель не предусмотрел таких понятий, как «электронная почта», «жесткий диск» или «источник компьютерной информации». На этом этапе судебная и следственная практика развивалась методом проб и ошибок, пытаясь втиснуть новые реалии в старые процессуальные формы.

Следователи и суды действовали по аналогии. Компьютерный системный блок или дискета изымались как вещественные доказательства по статье 83 УПК РСФСР. Содержащаяся на них информация рассматривалась не как самостоятельное доказательство, а как свойство данного предмета - подобно надписи на ноже или следам на одежде. Распечатки электронной переписки или данных из программ приобщались к делу как «иные

документы» (ст. 88 УПК РСФСР). Такой подход порождал системные проблемы, напрямую затрагивающие принципы процесса. Принцип законности нарушался из-за отсутствия четкой, предписанной законом процедуры: как именно изымать, упаковывать и хранить хрупкие электронные носители?[2] Принцип состязательности страдал, поскольку защита часто физически не могла получить копию доказательства в исходном цифровом виде для проведения своей экспертизы, работая лишь с бумажными распечатками. Принцип оценки доказательств по внутреннему убеждению суда ставился под сомнение, так как целостность данных (их неизменность с момента изъятия) никак не гарантировалась технически - не использовались хэш-суммы или цифровые подписи.

Второй этап (середина 2000-х – 2013 гг.): становление практики и первые ориентиры от высших судов. После введения в действие нового УПК РФ 2001 года и принятия базовых законов об информации (2006 г.) ситуация начала меняться. Законодатель по-прежнему молчал о специфике цифровых данных, но Верховный Суд РФ начал заполнять эти пробелы через канал судебной практики.

В обзорах и решениях ВС РФ стали появляться важные правовые позиции. Было, например, косвенно признано, что электронная переписка (из email, чатов) может служить доказательством, если надлежащим образом установлена принадлежность аккаунта конкретному лицу. Ключевую роль в легитимации цифровых улик стала играть судебная компьютерно-техническая экспертиза. Именно экспертиза превращала непонятные для суда байты данных в понятное заключение, которое можно было исследовать в суде, соблюдая принцип непосредственности. Однако фундаментальная проблема оставалась: отсутствие в УПК отдельной статьи о цифровых доказательствах означало, что их процессуальный статус был размыт и зависел от усмотрения правоприменителя. Следствие и суды по-прежнему вынуждены были «подгонять» цифровые данные под статьи о вещественных

доказательствах или документах, что не отражало их уникальной природы - легкости копирования, изменения и зависимости от средств воспроизведения.

Третий, переломный этап (2013 – 2020 гг.): законодательная формализация и новые вызовы. Ситуация кардинально изменилась с принятием Федерального закона от 04.03.2013 № 23-ФЗ, который ввел в УПК РФ специальную статью 81.1 «Электронные носители информации». Это стало революцией в процессуальном праве. Законодатель впервые признал специфику цифровых данных, разделив материальный носитель (флешка, жесткий диск) и информацию на нем как самостоятельный объект доказывания.

Статья 81.1 и последующие дополнения (ст. 164.1, 186.1 УПК РФ) установили детальную процедуру, направленную на обеспечение ключевых принципов:

Для законности был прописан четкий порядок изъятия ЭНИ с обязательным составлением протокола, фиксацией аппаратных характеристик и применением мер для сохранности данных.

Для состязательности появилась норма о возможности создания копии изъятой информации на носитель, предоставляемый защитой.

Для неприкосновенности частной жизни ввели судебный контроль за получением компьютерной информации у провайдеров (ст. 186.1).

Однако к 2020 году судебная практика выявила новые, еще более сложные проблемы, которые поставленные принципы вновь подвергли испытанию. Возникли вопросы о юрисдикции: как применять принцип непосредственности исследования доказательств, если данные физически хранятся в облачном сервере за границей? Как гарантировать неизменность доказательства, предъявленного в суде в виде скриншота из мессенджера? Как оценивать доказательства, добытые из зашифрованных устройств, что требует от суда специфических технических знаний, выходящих за рамки обычного внутреннего убеждения?[3]

Таким образом, к концу 2020 года развитие практики подошло к новому рубежу. Система прошла путь от полного игнорирования цифровых доказательств через этап судебной импровизации к их законодательному признанию и регламентации. Однако технологический прогресс - появление шифрования, облачных технологий, распределенных реестров - продолжил создавать вызовы для традиционных уголовно-процессуальных принципов. Практика 1990-2020 годов решила проблемы вчерашнего дня, создав фундамент, но одновременно обозначила контуры проблем завтрашнего, показав, что диалог между правом и технологиями является бесконечным процессом.

Несмотря на большой интерес исследователей к данному институту российского уголовного судопроизводства, пока невозможно с уверенностью сказать, что существует устоявшаяся и однозначно воспринимаемая в юридическом сообществе научная интерпретация электронных или, как их еще иногда называют, цифровых доказательств, а также внятная процессуальная процедура их собирания, проверки, оценки и использования.[4]

Такое положение в значительной степени обусловлено разборчивостью и осторожностью российского законодателя, который не спешит внедрять цифровые новшества в уголовное судопроизводство без должных гарантий прав его участников и обеспечения достоверности получаемых сведений, имеющих доказательственное значение. Однако важно не только обсуждать различные аспекты этой темы, но и апробировать новые информационные технологии в уголовном процессе, так как стремительное внедрение цифровизации во все сферы правоотношений стало насущной необходимостью, требуя адаптации российского уголовного судопроизводства к новым условиям.

Вместе с тем незыблемым остается то, что органу дознания, дознавателю, следователю и руководителю следственного органа необходимо

обнаруживать следы преступления, отображать их в собственном сознании, извлекать из них искомые сведения и фиксировать их в материалах уголовного дела в предусмотренной законом уголовно-процессуальной форме.

Например, если речь идет об идеальных следах, то они изначально должны найти отражение в сознании непосредственных участников преступления и его очевидцев, а затем сведущих лиц. Далее их показания, полученные в рамках производства соответствующих следственных действий, будут рассматриваться уполномоченными участниками уголовного судопроизводства на предмет наличия или отсутствия в них криминалистически значимой информации, потенциально способной трансформироваться в доказательства по уголовному делу.

В отличие от идеальных, материальные следы, отобразившиеся на тех или иных объектах мироздания, вначале должны быть обнаружены субъектами доказывания, зафиксированы, изъяты и только после этого с них может быть «считана» криминалистически значимая информация. В результате тщательного осмотра, процессуального оформления и принятия предусмотренного законом процессуального решения такие следы могут обрести статус доказательства.

Что касается виртуальных и цифровых следов, то местом их образования всегда является искусственная среда, именуемая киберпространством, а местом нахождения – память того или иного электронного устройства. Соответственно этому, криминалистически значимая информация, носителем которой оно является, также подлежит документальному оформлению, а ее электронный носитель должен пройти через призму личного восприятия с целью обретения статуса вещественного доказательства.

Развитие судебной и следственной практики работы с цифровыми доказательствами оказывает глубокое и неоднозначное влияние на

обеспечение принципов уголовного процесса. С одной стороны, оно служит их укреплению, а с другой - создает новые серьезные вызовы. Это развитие напрямую способствует законности, так как формирует единые и проверяемые стандарты для изъятия, фиксации и исследования цифровых данных. Суды и следствие вырабатывают четкие правила, что снижает произвол и субъективизм. Однако стремительная эволюция технологий постоянно опережает законодательство, создавая правовые пробелы, где принцип законности испытывает нагрузку.

Принцип осуществления правосудия только судом усиливается, поскольку суды становятся ключевыми арбитрами в оценке сложных цифровых доказательств. Именно судебная практика устанавливает критерии их допустимости и достоверности. Но здесь же кроется риск: техническая сложность материалов может привести к излишней зависимости суда от заключений узкоспециализированных экспертов, что косвенно может делегировать часть оценочной функции им.

Наиболее остро практика сталкивается с принципами уважения чести и достоинства личности и неприкосновенности частной жизни. Массовый сбор цифровых следов - метаданных, истории посещений, геолокации - создает угрозу тотальной слежки.[5] Следственная и судебная практика сегодня фактически определяют новые границы приватности в цифровую эпоху, решая, когда изъятие личной переписки или данных телефона соразмерно тяжести преступления. Аналогично трансформируется понимание неприкосновенности жилища - доступ к данным, хранящимся в «облаке» на зарубежных серверах, заставляет пересматривать традиционные юридические концепции.

Влияние на презумпцию невиновности и состязательность сторон двойственно. С одной стороны, цифровые доказательства могут стать мощным инструментом объективного установления истины, подтверждая или опровергая алиби. С другой - возникает опасный дисбаланс. Обвинение,

обладая государственными ресурсами и доступом к спецсредствам, часто имеет подавляющее преимущество в сборе и анализе таких доказательств. Защита же может быть лишена равных возможностей для их самостоятельной проверки из-за технической и финансовой сложности. Это подрывает реальную состязательность. Ответом практики на этот вызов становится развитие института судебной экспертизы по ходатайству защиты и более активное использование специалистов стороной защиты.

Таким образом, развитие практики работы с цифровыми доказательствами не просто адаптирует старые принципы к новым реалиям, а проводит их серьезную проверку на прочность. Оно требует от правоприменителя постоянного поиска баланса между эффективностью борьбы с преступностью и незыблемыми гарантиями прав личности, заложенными в основу уголовного процесса.

Список литературы:

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 21.04.2025) // Российская газета. 20001. № 249; Российская газета. 2025. № 93.

2. Качалова О.В., Цветков Ю.А. Электронное уголовное дело - инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. № 2. С. 95-101.

3. Воронин М.И. Электронные доказательства в УПК: быть или не быть // Науки криминального цикла. 2019. № 7 (152). С. 74–84.

4. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: автореф. дис. … канд. юрид. наук. М., 2020 [Электронный - 124 - ресурс]. URL: Вестник Тверского государственного университета. Серия «Право». 2024. № 4 (80)

5. Малышева О. А. Особенности доказывания, осуществляемого следователем, в условиях цифровизации уголовного судопроизводства // Вестник Университета имени О.Е. Кутафина. 2020. № 10 (74). С. 82-88.