Давыдова Алла Васильевна

декан

Северо-Западный институт (филиал)

АНО ВО «Московский гуманитарно-экономический университет»

г. Мурманск, Мурманская область

ЦИФРОВИЗАЦИЯ УГОЛОВНОГО ПРОЦЕССА КАК СОВРЕМЕННОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ПРОЦЕССА ДОКАЗЫВАНИЯ

Аннотация: *в статье раскрывается проблема специфики процедуры признания несостоятельным (банкротом) индивидуального предпринимателя. На основе анализа судебной практики выявляется тенденция признания судами допустимости доказательств, полученных с цифровых носителей, без получения судебной санкции на доступ к конфиденциальной информации. Автором обосновывается необходимость совершенствования уголовно-процессуального законодательства, включая введение нового понятия «получение доказательств в электронной форме» и детальную регламентацию процедур доступа к цифровым данным, содержащим личную переписку.*

Ключевые слова: *банкротство, кредитор, должник, неплатежеспособность, реестр, физические лица, задолженность, юридические лица.*

Современные реалии расследования и рассмотрения уголовных дел ставят перед уголовно-процессуальным законодательством новые, крайне актуальные вызовы. Эти вызовы напрямую связаны с активным и стремительным внедрением информационных технологий (IT) во все сферы правоприменительной практики. Важность использования IT-средств в уголовном процессе обусловлена прежде всего тем, что существующие правовые нормы, регулирующие применение цифровых технологий, зачастую не успевают за стремительным развитием и внедрением инноваций. Этот разрыв между технологическим прогрессом и законодательным регулированием порождает правовые коллизии и не всегда позволяет эффективно использовать потенциал IT для целей правосудия.

Наиболее значительное применение IT-технологии находят на ключевых этапах уголовного процесса.

1. Поиск и обнаружение доказательств. Использование цифровых инструментов для анализа больших объемов информации, поиска скрытых данных, отслеживания цифровых следов.

2. Изъятие доказательств. Осуществление законного и эффективного изъятия цифровой информации с различных носителей, включая компьютеры, мобильные устройства, облачные хранилища.

3. Фиксация доказательств. Обеспечение достоверности и юридической значимости цифровых доказательств, их надлежащая фиксация в соответствии с процессуальными требованиями.

Таким образом, интеграция IT в уголовный процесс становится не просто желательной, а необходимой мерой для повышения эффективности, оперативности и объективности расследований и судебных разбирательств. Однако, для полноценного использования этого потенциала требуется приведение законодательства в соответствие с современными технологическими реалиями. Они незаменимы при проведении сложных судебных экспертиз, а также при выполнении следственных и судебных действий, требующих высокой точности и оперативности.

Спектр возможностей, предоставляемых IT, чрезвычайно широк. С их помощью осуществляется мониторинг радиоэлектронной обстановки, проводится глубокий анализ массивов биллинговых данных, осуществляется снятие информации с технических каналов связи, детализируются телефонные соединения. Современные технологии позволяют получать высококачественные космические снимки, улучшать техническое качество фото- и видеоматериалов, проводить удаленный осмотр цифровых данных, хранящихся в сети Интернет, облачных хранилищах, а также в различных мессенджерах. Это значительно расширяет арсенал средств для сбора и анализа доказательственной информации [5].

Особое значение для развития дистанционных форм участия в уголовном процессе имеет Федеральный закон от 29.12.2022 №610-ФЗ [6], вступивший в

силу 9 января 2023 года. Данный закон существенно расширил возможности применения видеоконференцсвязи (ВКС) как для участия в судебных заседаниях, так и для получения доказательств. Применение ВКС стало возможным на всех стадиях уголовного процесса. Исключение составляют лишь заседания суда присяжных заседателей.

Однако, несмотря на широкое внедрение ВКС, понятие «видеоконференцсвязь» остается законодательно не определенным. Один документ, где содержится определение содержится видеоконференцсвязи, это Приказ Судебного департамента при Верховном Суде РФ от 28.12.2015 г. №401 [7]. Отсутствие четкого законодательного определения ВКС в основных процессуальных документах создает правовую неопределенность и потенциальные сложности в правоприменении.

Сбор цифровых доказательств в рамках уголовного судопроизводства представляет собой комплексный вызов, охватывающий правовые, технические аспекты и подбор адекватных методов. Одной из ключевых проблем, препятствующих эффективному использованию цифровых данных в уголовном процессе, является отсутствие четких и всеобъемлющих правил, регулирующих сам процесс получения этой информации. Существующие нормы зачастую не детализируют процедуры доступа к цифровым носителям и извлечения с них данных, что порождает неопределенность и потенциальные нарушения. Параллельно с этим, при доступе к цифровой информации остро встает актуальная проблема обеспечения незыблемости конституционных прав граждан. Речь идет о праве на следующее.

1. Неприкосновенность частной жизни – защита личного пространства от несанкционированного вторжения.

2. Защиту личной жизни – сохранение конфиденциальности личной информации и данных, касающихся частной жизни.

3. Тайну переписки и телефонных переговоров – гарантия конфиденциальности коммуникаций, включая SMS-сообщения, электронные письма и записи телефонных разговоров.

Огромное количество цифровых устройств – смартфонов, планшетов, компьютеров – изымается и подвергается осмотру в ходе уголовных расследований. Эти устройства, как правило, содержат колоссальный объем конфиденциальной информации, включая SMS-сообщения, личную переписку, фотографии, видео и другие данные, относящиеся к частной жизни граждан. Недостаточное законодательное регулирование процедур доступа к этим данным создает риск нарушения конституционных прав и свобод, требуя выработки более строгих и четких механизмов для балансирования интересов следствия и права на приватность.

Несмотря на важность соблюдения конституционных прав, судебная практика показывает, что получение санкции на доступ к таким сведениям с цифровых носителей является редким явным прецедентом. В правоприменительной практике зачастую наблюдается игнорирование потенциальных нарушений конституционных прав граждан.

Анализ судебной практики, в частности, протоколов осмотра цифровых устройств, использовавшихся подсудимыми для коммуникации, демонстрирует, как суды зачастую признают представленные доказательства допустимыми. Основная аргументация, используемая судами, как правило, сводится к тому, что доказательства были получены в соответствии с требованиями УПК РФ. Это включает в себя следующее.

1. Получение из достоверных источников. Утверждение, что информация извлечена из законно изъятого устройства.

2. Соблюдение всех процессуальных норм. Формальное выполнение требований закона, таких как наличие понятых при осмотре и фиксация обнаруженных данных.

Примерами такой практики служат приговоры Октябрьского районного суда г. Мурманска от 08.02.2024 по уголовному делу №1–11/2024 и Ленинского районного суда г. Мурманска от 20.02.2024 по уголовному делу №1–38/2024. В обоих случаях суды, несмотря на ходатайства защиты о признании представленных доказательств недопустимыми, пришли к выводу об их законности и относимости к делу.

Такая судебная практика вызывает серьезные вопросы и порождает правовые коллизии. Особую озабоченность вызывает тот факт, что доступ к информации, охраняемой законом как тайна, должен быть строго регламентирован и возможен только на основании судебного разрешения. Это особенно важно, учитывая существующие правовые нормы, которые уже регулируют доступ к другим видам конфиденциальных данных:

− почтово-телеграфные отправления (ст. 185 УПК РФ), доступ к ним требует судебного решения;

− контроль телефонных и иных переговоров (ст. 186 УПК РФ), данный вид контроля также осуществляется на основании судебного решения;

− информация о соединениях между абонентами (ст. 186.1 УПК РФ), получение такой информации также подчинено определенным процессуальным требованиям и, в ряде случаев, судебному контролю.

Отсутствие аналогичного строгого регламента для получения информации с цифровых устройств, содержащих личную переписку и другую конфиденциальную информацию, создает ситуацию, когда конституционные права граждан на тайну связи и неприкосновенность частной жизни могут оказаться ущемленными в угоду оперативности следствия. Необходима выработка четких законодательных механизмов, обеспечивающих баланс между потребностью в доказательствах и гарантией защиты прав личности.

Оценка цифровых доказательств связана с рядом существенных проблем, одной из которых является проверка их подлинности. Вопрос аутентичности данных ставится под сомнение, если существует вероятность их изменения, удаления или искажения.

Процесс проведения судебной экспертизы цифровых доказательств требует от специалистов высочайшей квалификации и глубокого понимания современных информационных технологий. Однако существующие стандарты нередко отстают от развития цифровой среды. Подробный анализ выявленных проблем и предложенных путей их решения представлен в Приложении А, таблице 1.

Для преодоления указанных трудностей предлагается рассмотреть целесообразность закрепления в УПК РФ нового понятия – «получение доказательств в электронной форме». Новая редакция предлагемой нормы: «Статья 186.2. «Получение доказательств в электронной форме». Данная норма должна детально регламентировать все этапы процесса, от инициации получения до фиксации и представления доказательств, обеспечивая при этом соблюдение прав участников уголовного судопроизводства и гарантируя достоверность и допустимость полученной информации (Приложение Б).

Совершенствование уголовно-процессуального законодательства в части использования цифровых способов передачи информации требует детального рассмотрения отдельных направлений. В первую очередь, это касается проблем, связанных с копированием и осмотром электронных сообщений. В условиях повсеместного доминирования цифровых форматов общения, закон до сих пор не содержит четко регламентированного следственного действия, которое бы позволяло эффективно получать информацию непосредственно из мессенджеров, электронной почты и социальных сетей, минуя необходимость изъятия физических носителей.

Несмотря на внесенные в ст. 185 УПК РФ изменения, существующая проблема остается нерешенной. Отсутствие разработанной процедуры осмотра и выемки электронных сообщений обусловлено тем, что положения, изложенные в частях 3–5 той же статьи, не учитывают специфику электронных сообщений и каналов их передачи [8]. Однако, при обмене сообщениями в сети Интернет-пользователи далеко не всегда используют свои реальные имена и фамилии, что, тем не менее, не препятствует их активному общению в мессенджерах. Это создает коллизию: законодателю необходимо сформулировать новые, более адаптированные признаки для индивидуализации субъекта, чьи электронные сообщения имеют значение для дела, когда реальные идентификаторы отсутствуют. Кроме того, п. 4 ч. 3 ст. 185 УПК РФ обязывает следователя указывать в ходатайстве наименование учреждения связи, ответственного за задержание почтово-

телеграфных отправлений. При этом Федеральный закон от 27 июля 2006 г. №149-ФЗ [9] не оперирует понятием «учреждение связи» в данном контексте.

Положения ч. 1 ст. 185 УПК РФ регламентируют право наложения ареста на «другие почтово-телеграфные отправления» при наличии достаточных оснований полагать, что они содержат сведения, имеющие значение для дела. Однако, неясно, охватывает ли это понятие электронные сообщения. Хотя Правила оказания услуг почтовой связи (п. 8) упоминают отправления, пересылаемые в форме электронного документа, и содержат положения о приеме и доставке таких отправлений, это касается лишь тех, что пересылаются с использованием информационной системы организации федеральной почтовой связи (п. 52). Таким образом, требуется четкое законодательное определение понятия «другие почтово-телеграфные отправления» в контексте цифровых коммуникаций.

Список литературы

1. Нилов К.Н. Унификация и дифференциация в правовом регулировании несостоятельности (банкротства) индивидуальных предпринимателей / К.Н. Нилов // Современные проблемы юридической науки и правоприменительной практики: сборник научных статей, посвященный 50-летию Юридического института БФУ им. И. Канта. – Калининград, 2017. – С. 127–135. EDN YSCZKP

2. По делу о проверке конституционности положений ст. 15 и 1064 Гражданского кодекса РФ, п. 1 ст. 9, п. 1 ст. 10 и п. 3 ст. 59 Федерального закона «О несостоятельности (банкротстве)» в связи с жалобой гражданина В.И. Лысенко: Постановление Конституционного Суда РФ от 18.11.2019 №36-П // Российская газета. – 2019. – №270 (29.11).

3. Постановление Пленума Верховного Суда РФ «О некоторых вопросах, связанных с введением в действие процедур, применяемых в делах о несостоятельности (банкротстве) граждан» от 13.10.2015 №45 // Российская газета. – 2015. – №235(19.10).

4. Сайфетдинова А.Ф. Особенности несостоятельности (банкротства) индивидуальных предпринимателей / А.Ф. Сайфетдинова, Т.И. Нестерова // Бюллетень науки и практики. – 2021. – Т. 7. №5. – С. 407–412. DOI 10.33619/2414-2948/66/42. EDN YWHMGU

5. Гришин А.В. Актуальные проблемы совершенствования уголовно-процессуального права в РФ / А.В. Гришин, О.Г. Селютина // Закон и право. – 2020. – №9. – С. 61–62. DOI 10.24411/2073-3313-2020-10422. EDN VQNXWA

6. Федеральный закон «О внесении изменений в Уголовно-процессуальный кодекс РФ» от 29.12.2022 №610-ФЗ // Российская газета. – 2023. – №2(10.01).

7. Приказ Судебного департамента при Верховном Суде РФ «Об утверждении Регламента организации применения видео-конференц-связи при подготовке и проведении судебных заседаний» от 28.12.2015 №401 (ред. от 30.12.2020) // Бюллетень актов по судебной системе. – 2016. – №3.

8. Супрун С.В. О противоречивом характере новеллы в законодательном регулировании следственного действия «наложение ареста на почтово-телеграфные отправления» / С.В. Супрун // Вестник Омской юридической академии. – 2017. – Т. 14. №1. – С. 62. DOI 10.19073/2306-1340-2017-14-1-59-64. EDN XWZCHF

9. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ (ред. от 24.06.2025) // Российская газета. – 2006. – №165(29.07).