Научная статья
УДК 343.14-028.27(470)

Ольга Вячеславовна Безлепкина[1], Анастасия Васильевна Федотова[2]
[1] Уфимский юридический институт МВД России, Уфа, Россия, oly-le@mail.ru
[2] Дальневосточный юридический институт МВД России имени И. Ф. Шилова, Хабаровск, Россия

ПРОБЛЕМНЫЕ АСПЕКТЫ СОБИРАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ

Аннотация. В свете цифровизации уголовного процесса вопрос о специфических видах доказательств приобретает новую значимость. Научное сообщество и практикующие юристы активно обсуждают целесообразность расширения существующей классификации доказательств, включив в нее «электронные доказательства». Пока теория доказательств в отношении к этому новому виду доказательств настроена скептически, но точка в научной дискуссии не поставлена, а законодательные вкрапления цифровых технологий в уголовное судопроизводство говорят о том, что практический запрос на новые теоретические положения весьма актуален. Практика ждет от науки принципиально новую трактовку электронных доказательств, не вписывающуюся в традиционные методологические схемы. Цель исследования заключается не только в анализе ключевых методов сбора цифровых доказательств, но и в выявлении существующих проблем в их обработке и применении. Исследование направлено на поиск эффективных решений этих проблем и предлагает пути совершенствования процессов работы с электронно-правовыми доказательствами. Особое внимание уделяется цифровым доказательствам как инструменту, позволяющему устанавливать юридически значимые факты в ходе уголовного судопроизводства.

Ключевые слова: электронные доказательства, преступление, компьютерные технологии, собирание доказательств, использование доказательств, доказывание, проверка доказательств

Для цитирования: Безлепкина О. В., Федотова А. В. Проблемные аспекты собирания электронных доказательств // Общество, право, государственность: ретроспектива и перспектива. 2025. № 2 (22). С. 25–35.

Original article

Olga V. Bezlepkina[1], Anastasia V. Fedotova[2]
[1] Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, oly-le@mail.ru
[2] Far Eastern Law Institute of the Ministry of Internal Affairs of Russia named after I. F. Shilov, Khabarovsk, Russia

PROBLEMATIC ASPECTS OF COLLECTING ELECTRONIC EVIDENCE

Abstract. In light of the digitalization of criminal proceedings, the issue of specific types of evidence is acquiring new significance. The scientific community and practicing lawyers are actively discussing the advisability of expanding the existing classification of evidence to include “electronic evidence”. While the theory of evidence is skeptical about this new type of evidence, the scientific discussion has not yet ended, and the legislative inclusion of digital technologies in criminal proceedings suggests that the practical demand

for new theoretical provisions is very relevant. Practice expects science to provide a fundamentally new interpretation of electronic evidence that does not fit into traditional methodological schemes. The purpose of the study is not only to analyze the key methods of collecting digital evidence, but also to identify existing problems in their processing and application. The study is aimed at finding effective solutions to these problems and suggests ways to improve the processes of working with electronic legal evidence. Particular attention is paid to digital evidence as a tool that allows establishing legally significant facts in the course of criminal proceedings.

Keywords: electronic evidence, crime, computer technology, collection of evidence, use of evidence, proving, verification of evidence

For citation: Bezlepkina O. V., Fedotova A. V. Problematic aspects of collecting electronic evidence // Society, law, statehood: retrospective and perspective. 2025. No. 2 (22). P. 25–35. (In Russ.)

Введение

Современная реальность неразрывно связана с цифровыми технологиями и глобальной сетью. Благодаря Интернету люди получили беспрепятственный доступ к колоссальным массивам информации различных форматов – от текстовых документов до разнообразного медиаконтента. Технологические корпорации-гиганты произвели настоящую революцию, создав «облачные» сервисы, которые превратили виртуальное пространство в надежное хранилище персональных данных каждого пользователя.

Цифровизация и технологический прогресс существенно трансформировали юридическую сферу, особенно в области уголовного права. Научное сообщество активно дискутирует о феномене цифровых следов – новой категории доказательств, появившейся вследствие повсеместного внедрения цифровых технологий.

Глобальные исследования демонстрируют, что использование компьютерных технологий в преступной деятельности становится распространенным явлением. Цифровые следы обнаруживаются при расследовании подавляющего большинства преступлений – согласно данным Совета начальников национальной полиции Великобритании, более 90 % случаев[1]. Эта закономерность прослеживается во всем мире, включая Россию. После сложных процедур обнаружения, документирования и извлечения эти цифровые следы трансформируются в полноценные доказательства, играющие ключевую роль в современном судопроизводстве.

Методы

В ходе научной работы был применен широкий методологический инструментарий. Обобщение, дедукция, индукция, синтез, анализ и сравнение составили основу общенаучного подхода. Исследование социально-правовой реальности дополнительно опиралось на специализированные методы: системно-структурный, историко-правовой, формально-юридический, а также моделирование.

Результаты

Прежде чем углубиться в анализ ключевых проблем, связанных с обнаружением и сбором цифровых доказательств, необходимо дать научное определение данному понятию.

В настоящее время уголовно-процессуальный закон не выделяет электронные (цифровые) доказательства в отдельный вид, а относит их к иным документам. Однако тенденция к выделению подобных доказательств в отдельный вид уже наметилась в Уголовно-процессуальном кодексе Российской Федерации (далее – УПК РФ). Так, в УПК РФ введена ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», которая закрепляет, что изъятие носителей цифровой информации должно осуществляться исключительно в присутствии специалиста.

[1] The National Policing Digital Strategy 2020–2030: Digital, Data and Technology Strategy (the Strategy). URL: https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf (дата обращения: 28.03.2025).

Часть 2 указанной статьи предусматривает условия и порядок копирования цифровой информации в ходе производства следственных действий[1].

Считаем, что все электронные доказательства можно разделить на электронные документы, электронные материалы, электронные сообщения и электронную переписку. В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, электронный документ – это документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах[2].

В. Ф. Янковая отмечает, что электронные документы представляют собой информационно-коммуникационное взаимодействие в цифровом формате, исключающее применение бумажных носителей, реализуется оно посредством особых информационных объектов [1, с. 230].

Н. Н. Ковалева и В. Ю. Коржов в своих исследованиях раскрывают электронный документ как комплекс взаимозависимых цифровых данных, существующих как в электронной, так и в цифровой среде, образуя единую информационную структуру[3].

И. Н. Подволоцкий детально анализирует роль цифровых материалов в доказательной базе. Автор предлагает широкую трактовку электронных документов, включая в них разнообразные формы представления информации – от традиционных текстовых файлов до мультимедийных материалов. Согласно его определению, к данной категории относятся любые данные, циркулирующие в информационно-телекоммуникационном пространстве, при условии их надлежащего процессуального оформления. Такие материалы, будь то схематические изображения, аудиозаписи, фотографические снимки или картографические данные, служат правоохранительным органам и суду инструментом для установления значимых обстоятельств в рамках уголовного судопроизводства [2, с. 34].

Законодательством установлены специальные критерии, которым должны соответствовать электронные документы для их признания допустимыми доказательствами в уголовном судопроизводстве:

1. Любые данные в цифровом формате должны быть строго ограничены информацией, имеющей прямое отношение к расследуемому делу [3, с. 189]. В частности, речь идет о фактических данных, указывающих на присутствие или отсутствие в поведении подозреваемого лица элементов противоправного действия, представляющего угрозу обществу.

2. При обмене документами через телекоммуникационные каналы или различные носители информации в электронном формате открываются значительные возможности. Однако ключевым вопросом становится подтверждение подлинности отправителя: необходимо достоверно убедиться, что документ действительно исходит от указанного лица [4, с. 247]. Важнейшим аспектом также является возможность проверки документа на предмет его целостности и отсутствия несанкционированных изменений. Поэтому система электронного документооборота обязательно должна включать механизмы, позволяющие проводить надежную идентификацию источника информации и верификацию неизменности содержания передаваемых данных.

3. Юридическая сила электронного документа как доказательства в суде воз-

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ // Собр. законодательства Рос. Федерации. 2001. № 52, ч. 1, ст. 4921.

[2] Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-Ф // Собр. законодательства Рос. Федерации. 2006. № 31, ч. 1, ст. 3448.

[3] Ковалева Н. Н. Информационное обеспечение органов власти : учеб. для вузов. 2-е изд., перераб. и доп. М. : Юрайт, 2025. С. 153.

никает исключительно при условии соответствия его оформления установленным уголовно-процессуальным нормам [5, с. 10].

Таким образом, исключительные характеристики электронных доказательств требуют их выделения в отдельную категорию в рамках УПК РФ. Это предполагает не только внесение четкого определения этих доказательств, включая их ключевые особенности, но и установление требования к проведению их экспертизы для подтверждения подлинности. Поэтому предлагаем в п. 63 ст. 5 УПК РФ закрепить понятие «электронные доказательства», под которыми следует понимать информацию, представленную в цифровой форме или хранящуюся на электронных устройствах, используемую участниками уголовного процесса для определения наличия или отсутствия обстоятельств, подлежащих доказыванию, и других значимых для расследования обстоятельств в ходе уголовного судопроизводства.

Уголовно-процессуальное законодательство изначально не предусматривало особенности правового регулирования процесса собирания цифровых доказательств. В. А. Новицкий указывает, что сегодня растет применение средств связи и последних технологических достижений для осуществления преступных действий. В свете того, как быстро техника входит в нашу жизнь, законодатели долгое время не спешили с адаптацией правовых норм к новым реалиям, в том числе к вопросам, касающимся использования цифровых данных в судебной практике [6, с. 216].

Федеральный закон № 143-ФЗ от 28 июля 2012 г.[1] внес изменения в УПК РФ, что стало первым шагом в адаптации законодательства к современным реалиям цифровой информации. До принятия этих поправок следователи и судьи были вынуждены расширительно интерпретировать процессуальные нормы, приспосабливая их к сбору электронных доказательств без учета специфики цифровых данных. В результате изменений был введен термин «электронный носитель информации». Однако законодатель не уточнил, что он подразумевает под этим термином, и не составил список возможных электронных устройств, которые могли бы подпадать под данное определение. Это привело к значительной неопределенности и стало причиной активных споров в научной среде.

Также для владельцев электронных данных при расследовании уголовных дел введены гарантии защиты их прав. Согласно обновленной ст. 81 УПК РФ, электронные устройства или носители информации, которые впоследствии не стали частью доказательств, должны быть возвращены владельцам. Кроме того, была введена ст. 81.1 УПК РФ, определяющая процедуру копирования данных с изъятых устройств по запросу их законных владельцев, что предусматривает новые меры по защите прав частных лиц и организаций, ставших участниками уголовного процесса. Важно подчеркнуть, что закон установил конкретные ограничения на запросы копирования информации, уточнив, что такие запросы допустимы только в определенных случаях, преимущественно связанных с преступлениями в предпринимательской сфере. Считаем абсолютно необоснованными существующие запреты, так как они не учитывают многочисленные ситуации, когда необходимо получить информацию с цифровых носителей. Защита законных интересов собственников документации может быть обеспечена только при условии предоставления им возможности дублировать требуемые электронные данные.

Изменилась процедура проведения следственных действий, в частности порядок обыска и выемки в соответствии с ч. 1 ст. 182 и ч. 2 ст. 183 УПК РФ. Теперь при работе с электронными носителями данных в рамках следственных действий обязательно должен присутствовать специалист.

[1] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 28 июля 2012 г. № 143-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Последующие и последние на данный момент изменения в УПК РФ, связанные с цифровизацией, были внесены законодателем в декабре 2018 г. Статья 164.1 УПК РФ соединила в себе особенности изъятия электронных носителей информации и копирования информации при производстве следственных действий, так как ранее соответствующие положения располагались отдельно в ст. 182, 183 УПК РФ, посвященных порядку проведения обыска и выемки[1].

Правовая норма об изъятии цифровых носителей с доказательствами имеет существенные недостатки, хотя для этой процедуры и был разработан отдельный юридический механизм [7, с. 110]. Детальное изучение данного положения выявляет его значительные изъяны. В соответствии с ч. 1 ст. 164.1 УПК РФ следственные органы обязаны иметь законные основания для сбора необходимых сведений. Получение необходимых сведений неприемлемо при отсутствии правовых оснований.

На практике сложно осуществить изъятие электронных носителей, даже при наличии процессуального документа. Постановление следственных органов (включая как следователей, так и дознавателей) о проведении судебной экспертизы цифровых накопителей является первичным правовым основанием, однако его недостаточно для эффективной реализации данного следственного действия. Согласно ч. 1 ст. 195 УПК РФ, перед проведением судебной экспертизы необходимо соблюсти ряд обязательных условий. Прежде всего следует полностью подготовить и укомплектовать материалы, которые будут подвергнуты экспертному анализу. Более того, уполномоченное лицо должно заранее четко сформулировать не только конкретный тип назначаемой экспертизы, но и составить исчерпывающий перечень вопросов, требующих профессионального экспертного заключения. Участникам уголовного процесса должны быть разъяснены их права согласно ч. 1 ст. 198 УПК РФ, а также обеспечена возможность их осуществления. Данное требование, наряду с ознакомлением заинтересованных лиц с постановлением о назначении экспертизы, является обязательным элементом соблюдения процедуры проведения судебной экспертизы.

Возможность реализации процессуальных прав участников производства и вынесение постановления о производстве судебной экспертизы напрямую зависят от существования электронных данных в материальной форме. В тех случаях, когда электронная информация не имеет физического носителя, становятся технически неосуществимыми как само оформление процессуального решения о назначении экспертизы, так и последующее ознакомление с ним заинтересованных лиц [8, с. 50]. Согласно правовому анализу, получить доступ к электронным данным и материалам следственные органы вправе посредством трех следственных действий, закрепленных в ч. 2 ст. 164.1 УПК РФ. Данные следственные действия включают выемку, осмотр места происшествия и обыск. При этом правовым основанием для осуществления копирования или изъятия информации с цифровых устройств должно служить наличие достаточной доказательственной базы, обосновывающей необходимость проведения указанных процессуальных действий.

Существует противоречие между нормами УПК РФ касательно изъятия электронных носителей. С одной стороны, ст. 164.1 УПК РФ вводит судебное решение как юридическое основание для такого изъятия. С другой стороны, это не соответствует положениям ст. 29 УПК РФ, которая ограничивает судебный контроль лишь теми процессуальными действиями, которые затрагивают конституционные права граждан. Такая несогласованность правовых норм вызывает обоснованные нарекания со стороны юридического сообщества и требует законодательного урегулирования. Судебное решение необходимо для проведения

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ // Собр. законодательства Рос. Федерации. 2001. № 52, ч. 1, ст. 4921.

ряда следственных действий, таких как обыск жилища, личный обыск или выемка документов, содержащих охраняемые законом сведения. Однако само по себе копирование данных с электронных устройств и их изъятие не входит в список процессуальных действий, требующих судебного контроля на этапе предварительного следствия. Представленный перечень не подлежит дополнениям и содержит исчерпывающую информацию. При этом правомерность работы с электронными носителями логически вытекает из наличия судебного разрешения на основное следственное действие, в рамках которого происходит изъятие предметов и документов.

Предлагаем внести изменения в ст. 29 УПК РФ: п. 14 ч. 2 ст. 29 УПК РФ, представив ее содержание в следующей формулировке, что «только суд, в том числе в ходе досудебного производства, правомочен принимать решения об изъятии электронных носителей информации при производстве по уголовным делам, указанным в части четвертой.1 статьи 164 УПК РФ».

В отдельном анализе нуждается и ч. 2 ст. 164.1 УПК РФ. Прежде всего обращает на себя внимание то обстоятельство, что законный владелец изымаемой информации вправе заявить ходатайство о ее копировании. Копирование осуществляется на другие электронные носители, предоставленные владельцем либо обладателем информации. Таким образом, следователь, согласно ч. 1 ст. 11 УПК РФ, должен не просто информировать участников процесса об их правах, но и создавать условия для их полноценной реализации. Однако существующий регламент фактически снимает с него обязательства по реализации этих прав. Более того, возможность копирования данных с изымаемых электронных носителей становится напрямую зависимой от наличия у их владельца альтернативных устройств хранения информации, что противоречит базовым процессуальным принципам.

Рассмотрим пример из судебной практики. В рамках ст. 125 УПК РФ были обжалованы процессуальные действия следователя. Содержание жалобы состояло в том, что при расследовании преступления следователем были организованы параллельные осмотры двух локаций – производственного цеха и офисного помещения предприятия. Такой подход сделал физически невозможным присутствие руководителя организации на обоих мероприятиях одновременно, что существенно ограничило его законные права, включая те, что закреплены в ч. 2 ст. 164.1 УПК РФ. При этом следствие не предложило альтернативного варианта в виде делегирования полномочий другому представителю администрации общества с ограниченной ответственностью для участия во втором осмотре. Суд вынес постановление об отказе в удовлетворении жалобы на действия сотрудников полиции при производстве осмотров места происшествия[1].

Таким образом, существующее правило по-прежнему дает возможность лицам, осуществляющим предварительное расследование, обходить установленные УПК РФ правила и запреты и фактически изымать электронные носители информации без реального предоставления их владельцам возможности скопировать необходимую информацию.

С целью решения указанной проблемы следует ч. 2 ст. 164.1 УПК РФ дополнить предложением: «Копирование информации осуществляется на другие электронные носители, предоставленные владельцем либо обладателем информации в течение 10 суток. При наличии уважительной причины неявки в указанный срок он может быть продлен до 30 суток».

При проведении досудебной проверки следователь имеет полномочия на изъятие электронных носителей во время осмотра места происшествия, что делает этот вопрос особенно актуальным. Опрос сотрудников следственных подразделений показал,

[1] Определение Третьего кассационного суда общей юрисдикции от 30 июня 2020 г. № 77-431/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

что правоохранители отдают предпочтение непосредственному изъятию цифровых устройств вместо копирования данных. Такой подход значительно ускоряет следственные мероприятия, избавляя от необходимости искать подходящие носители для дублирования информации и тратить время на сам процесс копирования (ст. 176, 177 УПК РФ). Складывается противоречивая ситуация: ч. 1 ст. 164.1 УПК РФ запрещает изъятие электронных носителей информации при производстве по уголовному делу, однако на стадии возбуждения уголовного дела, когда решение об уголовном преследовании еще не принято, изъятие электронных носителей допускается. Подтверждением этому служит судебная практика.

Так, в рамках проверки по заявлению о преступлении по ст. 171 Уголовного кодекса Российской Федерации правоохранительные органы произвели изъятие системного блока при осмотре места происшествия. Суд первой инстанции сделал вывод, что данное изъятие является незаконным, мотивируя это отсутствием установленного подозреваемого и неопределенной квалификацией деяния, что исключало применение положений ч. 1 ст. 164.1 УПК РФ. Однако суд кассационной инстанции не согласился с такой позицией и указал, что при наличии сообщения о преступлении осмотр места происшествия и изъятие значимых предметов являются законными следственными действиями, направленными на достижение конституционно значимых целей. Таким образом, кассационный суд признал правомерным как сам осмотр, так и изъятие компьютерного оборудования в его ходе[1].

Интерес вызывает обоснование применения ч. 3 ст. 164.1 УПК РФ, согласно которой следователь имеет право копировать данные с электронных носителей во время следственных действий.

Некоторые исследователи предлагают закрепить процедуру копирования цифровой информации в качестве самостоятельного следственного действия, так как сущность копирования цифровой информации значительно отличается от природы осмотра, обыска и выемки электронных носителей информации [9, с. 360]. Сохранение обнаруженного цифрового объекта в неизменном состоянии невозможно гарантировать полностью при простом копировании информации. Следовательно, мы считаем, что процесс копирования цифровых данных не следует классифицировать как самостоятельное следственное действие. Д. А. Степаненко указывает, что скопированную информацию сложно признать доказательством из-за утраты важных данных о точном времени и дате создания исходного файла при копировании. Такая проблема существенно осложняет доказательственный процесс [10, с. 27]. Из-за того, что простое копирование данных без извлечения электронного устройства, где они хранятся, может препятствовать полноценному расследованию обстоятельств дела, в уголовном процессе не принято рассматривать его как отдельное и самостоятельное следственное действие.

Таким образом, исходя из вышеизложенного, мы предлагаем внести изменения в ч. 3 ст. 164.1 УПК РФ, а именно дополнить ее предложением: «Физическое изъятие устройств хранения данных может быть произведено только при наличии судебного решения и достаточных оснований для возбуждения уголовного дела. В остальных случаях производится копирование информации».

Законодательство обязывает следственные органы предоставить собственнику или законному держателю цифровых данных все условия для создания резервной копии. В частности, необходимо выделить достаточный временной интервал для покупки подходящего носителя и осуществления процедуры дублирования контента с изымаемого устройства. Важно подчеркнуть, что процесс сбора цифровых данных выходит за рамки простого извлечения и копирования

[1] Определение Первого кассационного суда общей юрисдикции от 27 мая 2021 г. № 77-1475/2021. Доступ из справ.-правовой системы «КонсультантПлюс».

информации. К примеру, когда изымается компьютер для использования его данных в качестве доказательств в суде, это не означает, что можно без дополнительных объяснений предъявить само устройство или его содержимое на бумаге как доказательство. Для правоохранительных органов крайне важно детально описать процесс доступа к данным на электронных устройствах и методы их извлечения. Другими словами, необходимо осуществлять следственные действия (осмотр, выемка), целью которых является именно носитель информации, чтобы процедура копирования данных была законной. Исходя из анализа материалов следственной практики, можно сделать вывод о том, что почти в каждом третьем уголовном деле сотрудники правоохранительных органов осуществляют осмотр вещественных доказательств – электронных носителей информации с целью получения цифровой информации, то есть цифровых доказательств. Данное следственное действие производится в присутствии понятых и зачастую специалиста, результатом чего является копирование информации с электронного носителя [11, с. 290].

По смыслу ст. 176, 177 УПК РФ следственный осмотр представляет собой следственное действие, состоящее в непосредственном обозрении лицами, ведущими расследование, различных материальных объектов в целях выяснения обстановки совершения преступления, обнаружения и закрепления следов преступления, получения предметов, которые могут быть вещественными доказательствами, документов и установления иных обстоятельств, имеющих значение для уголовного дела[1].

В научном сообществе преобладает убеждение о необходимости внесения изменений в уголовно-процессуальное законодательство, предлагается ввести новый вид следственных действий как осмотр электронных данных, которые позволяли бы законно и эффективно извлекать цифровые данные из онлайн-систем с соблюдением технологических стандартов. Некоторые эксперты выдвигают предложение о добавлении в уголовно-процессуальное законодательство новой процедуры, названной «извлечение информации». Важно подчеркнуть, что детали и порядок выполнения этой процедуры остаются неопределенными, вызывая вопросы относительно жизнеспособности такого предложения [12, с. 67].

Некоторые эксперты предлагают использовать методы удаленного доступа для изыскания нужных данных, включая обход паролей и применение специализированного оборудования и программ [13, с. 83]. Однако этот подход подвергается критике, поскольку вмешательство в данные через такие методы может изменить их первоначальный вид, что впоследствии ставит под вопрос их пригодность в качестве доказательств. В аргументации противников этого метода особо подчеркивается, что специфика «удаленного обыска» влечет за собой не только выявление и сохранение информации, но и проникновение к ней, что неизбежно изменяет исходные данные, лишая их юридической значимости [14, с. 204].

Однако, несмотря на общее согласие о необходимости таких изменений, до сих пор не достигнут консенсус в том, какие именно процедуры должны быть официально утверждены в рамках уголовного процесса России для обеспечения правильного доступа к данным, хранящимся в электронной форме.

Заключение

Таким образом, в ходе исследования были выявлены следующие проблемы:

1. Наблюдается противоречие между нормами УПК РФ об изъятии электронных носителей: ст. 164.1 УПК РФ вводит судебное решение как юридическое основание для такого изъятия, что не соответствует положениям ст. 29 УПК РФ, которая ограничивает судебный контроль лишь теми процессуаль-

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ // Собр. законодательства Рос. Федерации. 2001. № 52, ч. 1, ст. 4921.

ными действиями, которые затрагивают конституционные права граждан. Данная проблема требует законодательного урегулирования.

Предлагаем внести изменения в ст. 29 УПК РФ, а именно в п. 14 ч. 2 ст. 29 УПК РФ закрепить, что «только суд, в том числе в ходе досудебного производства, правомочен принимать решения об изъятии электронных носителей информации при производстве по уголовным делам, указанным в части четвертой.1 статьи 164 УПК РФ».

2. Законный владелец изымаемой информации вправе заявить ходатайство о ее копировании на предоставленные им другие электронные носители. Следователь, согласно ч. 1 ст. 11 УПК РФ, должен не просто информировать участников процесса об их правах, но и создавать условия для их полноценной реализации. Однако существующий регламент фактически снимает с него обязательства по реализации этих прав. К тому же возможность копирования данных с изымаемых электронных носителей напрямую зависит от наличия у их владельца альтернативных устройств хранения информации, что противоречит базовым процессуальным принципам.

С целью решения указанной проблемы следует ч. 2 ст. 164.1 УПК РФ дополнить предложением: «Копирование информации осуществляется на другие электронные носители, предоставленные владельцем либо обладателем информации в течение 10 суток. При наличии уважительной причины неявки в указанный срок он может быть продлен до 30 суток».

3. Исследование материалов следственной практики выявило, что правоохранители отдают предпочтение непосредственному изъятию цифровых устройств вместо копирования данных. Это значительно ускоряет следственные мероприятия, избавляя от необходимости искать подходящие носители для дублирования информации и тратить время на сам процесс копирования (ст. 176, 177 УПК РФ). Складывается противоречивая ситуация: ч. 1 ст. 164.1 УПК РФ запрещает изъятие электронных носителей информации при производстве по уголовному делу, однако на стадии возбуждения уголовного дела, когда решение об уголовном преследовании еще не принято, изъятие электронных носителей допускается.

С целью решения данной проблемы предлагаем дополнить ч. 3 ст. 164.1 УПК РФ предложением: «Физическое изъятие устройств хранения данных может быть произведено только при наличии судебного решения и достаточных оснований для возбуждения уголовного дела. В остальных случаях производится копирование информации».

СПИСОК ИСТОЧНИКОВ

1. Янковая В. Ф. Электронный документ как объект документоведения // Вестник Волгоградского государственного университета. Сер. 2: Языкознание. 2013. № 3. С. 229–235.

2. Подволоцкий И. Н. Осмотр и предварительное исследование документов. М. : Юрлитинформ, 2004. 198 с.

3. Долгаев В. В. Электронные документы как доказательства в судебном процессе // Государственная служба и кадры. 2024. № 2. С. 188–191.

4. Карпушкина Г. В. Электронный документ как доказательство в уголовном процессе // Право, общество, государство: системные основы взаимодействия и развития : сб. статей научно-представительских мероприятий. М. : ИП Колупаева Елена Владимировна, 2024. С. 246–248.

5. Акименко А. А. Криминалистические проблемы сбора, проверки и оценки электронных документов как доказательств в уголовном судопроизводстве // Актуальные вопросы правоприменительной практики : по материалам симпозиума, Ростов-на-Дону, 24 окт. 2024 г. Ростов н/Д : Южный университет (ИУБиП), 2024. С. 8–13.

6. Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. № 1 (55). С. 213–221.

7. Шапиро И. М. Доказательственные критерии электронного документа в судопроизводстве // Вестник Дагестанского государственного университета. Сер. 3: Общественные науки. 2024. Т. 39, № 4. С. 109–117. DOI: https://doi.org/10.21779/2500-1930-2024-39-4-109–117

8. Буфетова М. Ш. Электронный документ как разновидность вещественных доказательств в российском уголовном судопроизводстве // Сибирские уголовно-процессуальные и криминалистические чтения. 2023. № 3 (41). С. 47–55. DOI: https://doi.org/10.17150/2411-6122.2023.3.47-55

9. Афанасьева С. И., Добровлянина О. В. О внедрении, развитии, усовершенствовании электронных способов собирания доказательственной информации по уголовным делам // Вестник Пермского университета. Юридические науки. 2023. Вып. 2 (60). С. 349–377. DOI: https://doi.org/10.17072/1995-4190-2023-60-349-377

10. Степаненко Д. А. Технология собирания электронно-цифровых доказательств: проблемы и рекомендации // ГлаголЪ правосудия. 2024. № 1 (35). С. 23–29.

11. Зайцев О. А., Пастухов П. С. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений // Вестник Пермского университета. Юридические науки. 2022. № 56. С. 281–308. DOI: https://doi.org/10.17072/1995-4190-2022-56-281-308

12. Орлова А. А., Муженская Н. Е. Использование информационных технологий в уголовном судопроизводстве: оптимизация правового регулирования // Законодательство. 2021. № 10. С. 65–70.

13. Шалумов М. С. Электронные доказательства в уголовном судопроизводстве // Уголовный процесс. 2021. № 12 (204). С. 80–85.

14. Дорошева А. А. Электронные «доказательства» в уголовном судопроизводстве Российской Федерации // Право и практика. 2019. № 4. С. 203–208.

REFERENCES

1. Yankovaya V. F. Electronic document as an object of record management // Science Journal of Volgograd State University. Linguistics. 2013. No. 3. P. 229–235. (In Russ.)

2. Podvolotsky I. N. Inspection and preliminary examination of documents. Moscow : Yurlitinform, 2004. 198 p. (In Russ.)

3. Dolgaev V. V. Electronic documents as evidence in court proceedings // Civil service and personnel. 2024. No. 2. P. 188–191. (In Russ.)

4. Karpushkina G. V. Electronic document as an evidence in criminal proceedings // Law, society, state: system foundations of interaction and development : a collection of articles of scientific and representative events. Moscow : individual entrepreneur Kolupaeva Elena Vladimirovna, 2024. P. 246–248. (In Russ.)

5. Akimenko A. A. Criminalistic problems of collection, verification and evaluation of electronic documents as an evidence in criminal proceedings // Topical issues of law enforcement practice : based on the materials of the symposium, Rostov-on-Don, October 24, 2024. Rostov-on-Don : Southern University (IMBL), 2024. P. 8–13. (In Russ.)

6. Novitsky V. A., Novitskaya L. Yu. Concept and types of digital evidence // Leningrad Law Journal. 2019. No. 1 (55). P. 213–221. (In Russ.)

7. Shapiro I. M. Evidentiary criteria for an electronic document in legal proceedings // Herald of Dagestan State University. Series 3: Social Sciences. 2024. Vol. 39, No. 4. P. 109–117. DOI: https://doi.org/10.21779/2500-1930-2024-39-4-109–117 (In Russ.)

8. Bufetova M. Sh. Electronic document as a type of physical evidence in Russian criminal proceedings // Siberian criminal procedure and criminalistic readings. 2023. No. 3 (41). P. 47–55. DOI: https://doi.org/10.17150/2411-6122.2023.3.47-55 (In Russ.)

9. Afanasyeva S. I., Dobrovlyanina O. V. On the introduction, development, improvement of electronic methods of collecting evidentiary information in criminal cases // Bulletin of Perm University. Juridical Sciences. 2023. Issue 2 (60). P. 349–377. DOI: https://doi.org/10.17072/1995-4190-2023-60-349-377 (In Russ.)

10. Stepanenko D. A. Technology for collecting electronic evidence: problems and recommendations // Glagol pravosidiya journal. 2024. No. 1 (35). P. 23–29. (In Russ.)

11. Zaitsev O. A., Pastukhov P. S. Digital face profile as an element of the information technology strategy for investigating crimes // Bulletin of Perm University. Juridical Sciences. 2022. No. 56. P. 281–308. DOI: https://doi.org/10.17072/1995-4190-2022-56-281-308 (In Russ.)

12. Orlova A. A., Muzhenskaya N. E. Use of information technologies in criminal proceedings: optimization of legal regulation // Legislation. 2021. No. 10. P. 65–70. (In Russ.)

13. Shalumov M. S. Electronic evidence in criminal proceedings // Criminal procedure. 2021. No. 12 (204). P. 80–85. (In Russ.)

14. Dorosheva A. A. Electronic "evidence" in criminal procedure of the Russian Federation // Law and practice. 2019. No. 4. P. 203–208. (In Russ.)

Информация об авторах:
Безлепкина О. В. – кандидат юридических наук, доцент;
Федотова А. В. – без ученой степени.

Information about the authors:
Bezlepkina O. V. – Candidate of Law, Associate Professor;
Fedotova A. V. – no academic degree.

Статья поступила в редакцию 23.04.2025; одобрена после рецензирования 30.04.2025; принята к публикации 20.06.2025.

The article was submitted 23.04.2025; approved after reviewing 30.04.2025; accepted for publication 20.06.2025.