

Научная статья
УДК 343.141, 343.131.3
DOI 10.33184/pravgos-2023.4.13

Original article

ГОЛОВАЧУК Ольга Сергеевна
Уральский государственный юридический
университет им. В.Ф. Яковлева,
Екатеринбург, Россия;
e-mail: persival@mail.ru;
<https://orcid.org/0000-0002-9331-4046>

GOLOVACHUK Olga Sergeevna
Ural State Law University named after
V.F. Yakovlev, Yekaterinburg, Russia.

РАМЕНСКАЯ Виктория Святославовна
Уральский государственный юридический
университет им. В.Ф. Яковлева,
Екатеринбург, Россия;
e-mail: viva-ra@mail.ru;
<https://orcid.org/0000-0003-0428-7283>

RAMENSKAYA Victoria Svyatoslavovna
Ural State Law University named after
V.F. Yakovlev, Yekaterinburg, Russia.

ПУТИ СОВЕРШЕНСТВОВАНИЯ ИНСТИТУТА ДОКАЗАТЕЛЬСТВЕННОГО ПРАВА В УГОЛОВНОМ ПРОЦЕССЕ РОССИИ В СВЕТЕ ЦИФРОВИЗАЦИИ

WAYS TO IMPROVE THE INSTITUTE OF EVIDENTIARY LAW IN RUSSIAN CRIMINAL
PROCEDURE IN THE LIGHT OF DIGITALIZATION

Аннотация. С момента вступления в силу УПК РФ прошло уже более 20 лет. За указанный период окружающий мир претерпел значительные изменения. Речь, прежде всего, идет о так называемом процессе цифровизации, когда электронная среда все активнее охватывает различные сферы жизни, в том числе уголовное судопроизводство. Можно говорить о двух основных направлениях. Во-первых, информация, имеющая доказательственное значение в рамках производства по делу, довольно часто содержится на электронных носителях: флэш-картах, сим-картах, жестких дисках и т. д. Во-вторых, меняются способы передачи информации. Это требует от законодателя внесения соответствующих изменений в УПК РФ, в частности, это касается норм, регулирующих процесс доказывания по уголовным делам. Цель: анализ проблем применения уголовно-процессуального законодательства, регулирующего процесс доказывания, в условиях цифровизации и поиск путей их решения. Методы: сравнения и интерпретации, формальной и диалектической логики, толкования юридических норм. По результатам проведенного исследования обоснована необходимость закрепления в УПК РФ таких следственных действий, как копирование и осмотр электронных сообщений, выемка информации в цифровой форме, находящейся в виртуальных хранилищах, а также необходимость нормативного определения понятия «электронный носитель информации». Кроме того, следует предусмотреть дополнительные меры по защите сведений, копируемых и хранящихся в цифровой форме на электронных устройствах сотрудников правоохранительных органов, в ходе расследования уголовных дел.

Abstract. More than 20 years have passed since the Code of Criminal Procedure of the Russian Federation entered into force. During this period, the world has undergone significant changes. The first is the so-called digitalization process, when the electronic environment is increasingly covering various spheres of life, including criminal proceedings. There are two main directions. Firstly, information of evidentiary value in the proceedings is quite often contained on electronic media: flash cards, SIM cards, hard disks, etc. Secondly, the methods of transmitting this information are also changing. This requires the legislator to make appropriate amendments to the Code of Criminal Procedure of the Russian Federation; in particular, this concerns the rules governing the process of proving in criminal cases. Purpose: to analyze the problems in the application of criminal procedural legislation governing the process of proving in the conditions of digitalization and to find ways to solve them. Methods: methods of comparison and interpretation; methods of formal and dialectical logic; interpretation of legal norms. Results: the study substantiates the necessity of fixing in the Criminal Procedure Code of the Russian Federation such investigative actions as copying and inspection of electronic messages, seizure of information in digital form located in virtual storages, as well as a regulatory definition of the concept of «electronic storage medium». In addition, further measures should be provided to protect information copied and digitally stored on electronic devices of law enforcement officers during criminal investigations.

© Головачук О.С., Раменская В.С., 2023

Ключевые слова: следственные действия, передача информации, информационно-телекоммуникационная сеть, электронный носитель информации, цифровизация, электронные сообщения

Для цитирования: Головачук О.С. Пути совершенствования института доказательственного права в уголовном процессе России в свете цифровизации / О.С. Головачук, В.С. Раменская. – DOI 10.33184/pravgos-2023.4.13 // Правовое государство: теория и практика. – 2023. – № 4. – С. 113–119.

Keywords: investigative actions, information transfer, information and telecommunication network, electronic storage medium, digitalization, electronic messages

For citation: Golovachuk O.S., Ramenskaya V.S. Ways to improve the institute of evidentiary law in Russian criminal procedure in the light of digitalization. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2023, no. 4, pp. 113–119 (In Russian). DOI 10.33184/pravgos-2023.4.13.

ВВЕДЕНИЕ

В последние десятилетия результаты научно-технического прогресса настолько прочно вошли в нашу жизнь, что ее уже невозможно представить без оперативного доступа к информации, возможности мгновенно передавать сведения в любую часть Земли практически неограниченному числу людей, фиксировать все происходящее с помощью фото-, видео-, аудиотехники. При этом носители информации становятся все более компактными и удобными в использовании. Данные процессы стали возможны благодаря цифровизации.

Существуют два основных способа передачи информации: цифровой и аналоговый. В последнем случае информация передается непрерывно и так же должна восприниматься. Аналоговые сигналы раньше использовались во всех видах связи, но постепенно они вытесняются цифровыми, так как информация передается практически без искажений и требует минимальных затрат энергии для ее приема и передачи¹.

Данные изменения носят глобальный характер и влияют на самые разные области деятельности человека, в том числе входящие в сферу правовой регламентации.

Не осталось в стороне и уголовное судопроизводство. Но если сравнивать его с гражданским и арбитражным процессами, то можно сделать вывод, что изменения происходят более плавно, даже осторожно. Причины кроются в том числе и в тех итоговых решениях,

которые принимаются по результатам рассмотрения уголовных дел, в их влиянии на жизнь многих участников уголовного процесса. Тем не менее современные технологии передачи данных все больше проникают и в уголовное судопроизводство.

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА СИСТЕМУ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Для начала следует разобраться с терминологией. Многие авторы настаивают на использовании термина «цифровой» (в частности, в последние годы появился и активно развивается новый раздел криминалистики – криминалистическое исследование компьютерных средств и систем, активно обсуждаются вопросы цифровизации судебно-экспертной деятельности [1, с. 9]), но законодатель в различных нормативных актах оперирует категорией «электронный». Обратимся к закону «Об информации, информационных технологиях, защите информации»², согласно ст. 2 которого под информацией следует понимать сведения (сообщения, данные) вне зависимости от формы их предоставления. В данной норме приведено определение электронного сообщения: информация, переданная или полученная пользователем информационно-телекоммуникационной сети, то есть технологической системы, предназначенной для передачи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Нет сомнений, что информация при этом передается в форме

¹ Аналоговый и цифровой сигнал. Типы сигналов и как это действует [Электронный ресурс] // Электросам.ру : информационно-познавательный сайт. URL: <https://electrosam.ru/glavnaja/jelektrotehnika/raschjoty/analogovyi-i-tsifrovoyi-signal/> (дата обращения: 23.08.2023).

² Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 31.07.2023) [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 13.09.2023).

цифрового кода, самый простой из которых – последовательно сменяемые «0» и «1», то есть, по сути, эта информация является цифровой. Тем не менее УПК РФ в ст. 474.1 использует термин «электронные документы», которые передаются в информационно-телекоммуникационной сети Интернет. В ст. 189.1 и 278.1 упоминается возможность использования видео-конференц-связи, но через какие каналы будет осуществляться передача информации, в законе не сказано. Можно предположить, что речь идет об использовании цифровых способов передачи информации через Интернет. Поэтому в настоящей работе применительно к информации, ее форме и носителям наряду с термином «цифровой» будет использоваться термин «электронный».

Передача информации сопровождает все уголовное судопроизводство. Но особое значение она имеет в рамках процесса доказывания. Ведь именно в данном случае информация в самых разнообразных формах доводится до сведения одного участника другим участником. При этом процедура передачи сведений максимально формализована, особые требования предъявляются к их форме и участникам. Нет достоверных данных в пользу того, что законодатель в обозримом будущем готов будет изменить порядок доказывания при разбирательстве уголовных дел. Поэтому следует говорить об адаптации появившихся способов передачи данных под нормативно предъявляемые доказательственным правом требования.

Мы проанализируем несколько направлений, в рамках которых необходимо совершенствование действующего уголовно-процессуального законодательства, обусловленное использованием цифровых способов передачи информации. Прежде всего, хотелось бы обратиться к следственным действиям. Их перечень строго регламентирован законом и является закрытым, но при пристальном рассмотрении становится ясно, что он нуждается в корректировке.

КОПИРОВАНИЕ И ОСМОТР ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Общение в цифровом формате все более вытесняет иные способы передачи информации. Как же законодатель учитывает ука-

занное обстоятельство при регулировании процедуры собирания необходимых для рассмотрения дела фактических данных?

В законе отсутствует следственное действие, которое бы позволяло получить, в том числе минуя носитель, принадлежащую конкретному лицу информацию из мессенджеров, электронных ящиков, социальных сетей. Изменения, внесенные законодателем в ст. 185 УПК РФ, не решили существующую проблему. Указанная статья была дополнена частью 7, в соответствии с которой следователь по решению суда может произвести осмотр и выемку электронных и иных передаваемых по сетям электросвязи сообщений при наличии достаточных оснований полагать, что в них содержатся сведения, имеющие значение для уголовного дела. При этом мы видим, что процедура такого осмотра и выемки не разработана, так как правила, изложенные в ч. 3–5 ст. 185 УПК РФ, не учитывают специфики электронных сообщений и каналов их передачи. Так, например, в ходатайстве следователя о наложении ареста на почтово-телеграфные отправления обязательно указываются данные лица, на чье имя поступают эти отправления (его фамилия, имя, отчество и адрес). Но при обмене сообщениями в сети Интернет далеко не всегда используются настоящие имена и фамилии, что не является препятствием для общения посредством мессенджеров. Соответственно, законодателю необходимо сформулировать иные признаки, которые позволят индивидуализировать субъекта, чьи электронные сообщения содержат информацию, имеющую значение для уголовного дела [2, с. 62]

Также п. 4 ч. 3 ст. 185 УПК РФ требует от следователя указать в своем ходатайстве наименование учреждения связи, на которое возлагается обязанность задерживать соответствующие почтово-телеграфные отправления. Но Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» не использует такого понятия. Соответственно, возникают вопросы: от кого следователь может получить интересующие его электронные сообщения с целью их копирования и осмотра? насколько корректно решение законодателя о включении нормы ч. 7 ст. 185 УПК РФ в статью, посвященную аресту, выемке и осмотру почтово-телеграфных отправок?

В соответствии с ч. 1 ст. 185 УПК РФ на бандероли, посылки или другие почтово-телеграфные отправления либо телеграммы и радиogramмы может быть наложен арест при наличии достаточных оснований полагать, что в них содержатся предметы, документы или сведения, имеющие значение для уголовного дела. При этом не понятно, что включает в себя понятие «другие почтово-телеграфные отправления», охватываются ли его содержанием электронные сообщения.

Так, п. 8 Правил оказания услуг почтовой связи, утвержденных приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 17 апреля 2023 г. № 382³, среди почтовых отправлений упоминает отправление, пересылаемые в форме электронного документа, а в разделе VI содержатся положения о приеме и доставке (вручении) простых и заказных почтовых отправлений, пересылаемых в форме электронного документа. Но речь здесь идет только об отправлениях, пересылаемых с использованием информационной системы организации федеральной почтовой связи (п. 52). Таким образом, можно сделать вывод, что электронные и иные передаваемые по сетям электросвязи сообщения выходят за рамки предмета ст. 185 УПК РФ, так как к ним относятся сообщения, передаваемые по электронной почте, а также посредством мессенджеров (WhatsApp, Viber, Telegram и др.).

Учитывая изложенное, следует согласиться с теми учеными-процессуалистами, которые говорят о необходимости закрепления в УПК РФ самостоятельного следственного действия, направленного на копирование и осмотр электронных сообщений [3, с. 479–480].

Но это в полной мере не решит проблему взаимодействия правоохранительных органов с организаторами распространения электронной информации по сети Интернет, если последние находятся за пределами Российской Федерации. Как справедливо отмечают В.В. Важенин и Т.З. Имаков, «большинство протоколов и технологий сети Интернет разработаны в США. Корпорации по управлению доменными именами и IP-адресами (ICANN) созданы при участии американского правительства и находятся на территории США» [4, с. 21].

³ Правила оказания услуг почтовой связи, утв. приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 17.04.2023 № 382 [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 13.09.2023).

ЭЛЕКТРОННЫЕ УСТРОЙСТВА КАК НОСИТЕЛИ ИНФОРМАЦИИ

Также в рамках исследуемой темы требует внимания вопрос об электронных устройствах как носителях информации и приобщении их в качестве доказательств. Законодателем уже предприняты определенные шаги в данном направлении. Так, в УПК РФ появилась ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий». При этом законодатель не посчитал необходимым закрепить в тексте процессуального закона определение понятия «электронные носители информации». Поэтому на практике приходится использовать ГОСТ 2.051-2013 «Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения»⁴, в п. 3.1.9 которого говорится, что электронный носитель – это материальный носитель, используемый для записи, хранения и воспроизведения информации с помощью средств вычислительной техники. Следует отметить расплывчатость приведенной формулировки, что обуславливает вариативность восприятия понятия «электронный носитель» [5, с. 117]. На практике это может привести к необоснованному отказу в отнесении того или иного устройства к электронным носителям информации и, как следствие, к несоблюдению установленных законом процедур, нарушению прав участников уголовного судопроизводства [6, с. 67]. Таким образом, полагаем, что ст. 5 УПК РФ, раскрывающую определение основных понятий, используемых в тексте уголовно-процессуального закона, следует дополнить пунктом 63, указав, что электронный носитель информации – это предмет, используемый для записи, постоянного или временного хранения электронной информации, имеющей значение для уголовного дела, воспроизведение которой невозможно без использования вычислительной техники.

⁴ ГОСТ 2.051-2013. «Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения» [Электронный ресурс] // доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 13.09.2023).

ПРОБЛЕМЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ

Сама норма, регламентирующая порядок производства данного следственного действия, появилась в законе в 2010 г., последние изменения и дополнения были внесены в нее в 2013 г. Очевидно, что с тех пор возможности цифровых технологий, электронных устройств и степень их распространенности среди населения шагнули далеко вперед. Многие авторы отмечают ряд пробелов в действующей норме: не регламентированы основания производства следственного действия, не определен процессуальный статус лиц, в отношении которых оно может быть произведено; императивность правила о признании вещественным доказательством полученной в ходе указанного действия информации также вызывает сомнения [7, с. 82]. Кроме того, не урегулирован порядок взаимодействия следственных органов и операторов связи, не установлена ответственность за нарушение обязательств операторов связи в рамках выполнения судебного решения на производство следственного действия и др. [8, с. 55].

Также потенциально важным видится получение информации как о факте соединения между абонентами (абонентскими устройствами), объеме передаваемых сведений, так и о том, какие именно сведения были переданы, в каких программах состоялась передача. Тем более что с принятием ряда федеральных законов⁵ предпосылки для этого в виде обязательного хранения операторами связи передаваемых сведений уже созданы.

⁵ О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»: Федеральный закон от 06.07.2016 № 374-ФЗ (последняя редакция) [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 13.09.2023); О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 06.07.2016 № 375-ФЗ (последняя редакция) [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 13.09.2023).

ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ДОКАЗЫВАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ

Как уже было отмечено, цифровые технологии позволяют оперативно собирать и передавать информацию в самых разных форматах. При этом в уголовно-процессуальном законе не регламентированы виды технических средств, подлежащих применению для фиксации хода и результатов следственного действия. Статья 164 УПК РФ содержит на этот счет лишь самые общие правила. Поэтому представители правоохранительных органов используют личные технические средства. Прежде всего, речь идет о смартфонах. Конечно, это удобно: оперативная фиксация, нужные сведения всегда под рукой. Оснований сомневаться в добросовестности сотрудников правоохранительных органов, прокуратуры и других ведомств нет. Поэтому в настоящей работе даже не обсуждается возможность умышленной передачи сведений третьим лицам. Но есть еще и техническая возможность неправомерного и неконтролируемого доступа к информации, хранящейся на устройствах сотрудников, имеющих доступ в Интернет. Кроме утечки есть вероятность неправомерного получения данных, хранящихся на личных устройствах, подключенных к Сети, их изменения и неконтролируемого владельцем возвращения фото, аудио или иного файла на устройство. В этой связи предлагается более детально регламентировать порядок хранения и передачи информации, прежде всего, при расследовании уголовных дел и рассмотрении некоторых из них в закрытом судебном разбирательстве. Необходимо нормативно запретить использование личных устройств сотрудников, подключенных к Интернету, либо предусмотреть дополнительные механизмы защиты от неправомерного проникновения к информации, хранящейся на них. Важно не просто установить указанные ограничения, но и проконтролировать их соблюдение, ввести санкции за их игнорирование. Возможно, данное предложение на первый взгляд может показаться излишним, поскольку подобные случаи пока не были описаны в открытой печати. Но необходимо действовать на опережение, ведь последствия описанных неправомерных действий могут быть фатальными.

ми для разбирательства уголовных дел при действующем принципе презумпции невиновности, особенно если информация не была продублирована в первоначальном виде на устройствах, не подключенных к Интернету, или на бумажном носителе.

Уголовно-процессуальный порядок предоставления информации с электронных носителей участниками уголовного судопроизводства

Хотелось бы обратить внимание на отсутствие правового обеспечения тех случаев, когда участники процесса предоставляют лицам, ведущим производство по уголовному делу, цифровую информацию на личных устройствах. В частности, такая необходимость может возникнуть при производстве допроса или участия в иных следственных действиях. УПК РФ предусматривает в указанных случаях возможность производства выемки. Но если информация находится в цифровом виде, то могут возникнуть вопросы в связи с ее копированием на материальный носитель и приобщением к уголовному делу: кто именно, с помощью каких устройств осуществит копирование, кто должен предоставить носитель для переноса информации и др. Эти вопросы также требуют нормативных ответов. Важно отметить, что ст. 164.1 УПК РФ регламентирует, прежде всего, процедуру изъятия электронного носителя информации. Но необходимость изъятия сведений, содержащихся в виртуальных цифровых хранилищах, только возрастает. Зайти в такие хранилища можно с любого электронного устройства при введении логина и пароля. Очевидно, что изъятия конкретного устройства, на котором хранится информация, в данном случае не требуется. В этой связи предлагается включить в УПК РФ статью 183.1, наделив субъекта, предоставляющего сведения в цифровом виде, правом выбирать: либо скопировать важную для разбирательства дела информацию самостоятельно на свой носитель с последующей его передачей для хранения при уголовном деле и компенсацией затрат, либо обратиться к соответствующим специалистам, работникам правоохранительных органов. В случае принятия данного предложения необходимо создать соответствующие подразделения в правоохранительных органах и судах. На

них могут быть возложены и иные функции. Например, производство экспертиз носителей цифровой информации или помощь в их назначении, осмотре указанных предметов.

При этом использование цифровой информации в процессе доказывания по уголовному делу может вестись и в других направлениях. Для этого необходимо нормативно закрепить соответствующие дополнения к уголовно-процессуальной форме, расширив пределы допустимости использования цифровых источников фактических данных, изменить систему принципов уголовного процесса, расширить перечень не только следственных, но и судебных действий [9, с. 55].

ЗАКЛЮЧЕНИЕ

Подводя итоги проведенного исследования, можно сделать следующие выводы:

1) в тексте УПК РФ (ст. 5) необходимо закрепить понятие «электронный носитель информации»;

2) следует предусмотреть в действующем уголовно-процессуальном законодательстве самостоятельное следственное действие – копирование и осмотр электронных сообщений, – исключив ч. 7 ст. 185 УПК РФ;

3) полагаем возможным расширить перечень сведений, которые могут быть получены в рамках производства следственного действия, предусмотренного ст. 186. 1 УПК РФ;

4) необходимо предпринять повышенные меры безопасности, обеспечивающие сохранность и контроль за информацией, хранящейся в цифровой форме на личных устройствах сотрудников правоохранительных органов. В этой связи предлагается разработать и установить на личных устройствах сотрудников программы, обеспечивающие сохранность информации и запрещающие неправомерный доступ к ней с других устройств;

5) необходимо дополнить УПК РФ статьей 183.1, в которой закрепить право участника уголовного судопроизводства, предоставляющего сведения в цифровом виде, выбирать: либо скопировать имеющую значение для дела информацию самостоятельно на свой носитель с последующей его передачей для хранения при уголовном деле и компенсацией затрат, либо обратиться к соответствующим специалистам, работникам правоохранительных органов.

СПИСОК ИСТОЧНИКОВ

1. Россинская Е.Р. Учение о цифровизации судебно-экспертной деятельности и проблемы судебно-экспертной дидактики / Е.Р. Россинская // Правовое государство: теория и практика. – 2020. – № 4, ч. 1. – С. 88–101.
2. Супрун С.В. О противоречивом характере новеллы в законодательном регулировании следственного действия «наложение ареста на почтово-телеграфные отправления» / С.В. Супрун, В.С. Черкасов // Вестник Омской юридической академии. – 2017. – Т. 14, № 1. – С. 59–64.
3. Гарипов Т.И. Вопросы процессуальной регламентации копирования и осмотра электронных сообщений в уголовном судопроизводстве / Т.И. Гарипов // Вестник Казанского юридического института МВД России. – 2019. – № 4 (38). – С. 475–481.
4. Важенин В.В. Проблемы противодействия экстремизму в сети Интернет / В.В. Важенин, Т.З. Имаков // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2015. – № 1. – С. 19–26.
5. Количенко А.А. Электронные носители информации как средство получения электронных доказательств в уголовном процессе / А.А. Количенко // Вестник Казанского юридического института МВД России. – 2022. – № 1 (47). – С. 114–121.
6. Григорьев В.Н. Об электронных носителях информации в уголовном судопроизводстве / В.Н. Григорьев, О.А. Максимов // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2019. – № 3. – С. 65–71.
7. Сибигатуллин Ф.Ф., Латыпов В.С. И снова к вопросу о получении информации о соединениях между абонентами и (или) абонентскими устройствами / Ф.Ф. Сибигатуллин, В.С. Латыпов // Общество, право, государственность: ретроспектива и перспектива. – 2021. – № 2. – С. 78–83.
8. Сандрин И.А. Взаимодействие органов предварительного следствия и операторов связи при расследовании дистанционных мошенничеств / И.А. Сандрин, В.А. Мещеряков // Вестник Краснодарского университета МВД России. – 2022. – № 3 (57). – С. 51–56.
9. Зайцев О.А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства / О.А. Зайцев // Журнал зарубежного законодательства и сравнительного правоведения. – 2019. – № 4. – С. 42–57.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Головачук Ольга Сергеевна – кандидат юридических наук, доцент кафедры судебной деятельности и уголовного процесса;

Раменская Виктория Святославовна – кандидат юридических наук, доцент кафедры судебной деятельности и уголовного процесса.

INFORMATION ABOUT THE AUTHOR

Golovachuk Olga Sergeevna – Candidate of Sciences (Law), Assistant Professor of the Department of Judicial Activity and Criminal Procedure;

Ramenskaya Victoria Svyatoslavovna – Candidate of Sciences (Law), Assistant Professor of the Department of Judicial Activity and Criminal Procedure.

Статья поступила в редакцию 29.10.2023; одобрена после рецензирования 26.11.2023; принята к публикации 27.11.2023. The article was submitted 29.10.2023; approved after reviewing 26.11.2023; accepted for publication 27.11.2023.

REFERENCES

1. Rossinskaya E.R. The doctrine of forensic activities digitalization and the problems of forensic didactics. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2020, no. 4, pt. 1, pp. 88–101. (In Russian).
2. Suprun S.V., Cherkasov V.S. On the opposing nature of novella in the legislative regulation of the investigatory action «arrest of postal and telegraph». *Vestnik Omskoj yuridicheskoy akademii = Siberian Law Review*, 2017, vol. 14, no. 1, pp. 59–64. (In Russian).
3. Garipov T.I. Procedural regulation of copying and inspection of electronic messages in criminal court proceedings. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA of Russia*, 2019, no. 4 (38), pp. 475–481. (In Russian).
4. Vazhenin V.V., Imakov T.Z. Problems of countering extremism on the Internet. *Prestupnost' v sfere informacionnyh i telekommunikacionnyh tekhnologij: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenij = Crime in the field of information and telecommunication technologies: problems of prevention, detection and investigation of crimes*, 2015, no. 1, pp. 19–26. (In Russian).
5. Kolichenko A.A. Electronic media as a source of obtaining electronic evidence in criminal proceedings. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA of Russia*, 2022, no. 1 (47), pp. 114–121. (In Russian).
6. Grigoryev V.N., Maksimov O.A. On the use of electronic storage media in criminal proceedings. *Vestnik Nizhegorodskogo universiteta imeni N.I. Lobachevskogo = Vestnik of Lobachevsky University of Nizhni Novgorod*, 2019, no. 3, pp. 65–71. (In Russian).
7. Sibagatullin F.F., Latypov V.S. Getting back to the issue of obtaining information on connections between subscribers and (or) subscriber devices. *Obshchestvo, pravo, gosudarstvennost': retrospektiva i perspektiva = Society, Law, Statehood: Retrospective and Perspective*, 2021, no. 2, pp. 78–83. (In Russian).
8. Sandrin I.A., Meshcheryakov V.A. Interaction of preliminary investigation bodies and telecom operators in the investigation of remote fraud. *Vestnik Krasnodarskogo universiteta MVD Rossii = Bulletin of Krasnodar University of Russian MIA*, 2022, no. 3 (57), pp. 51–56. (In Russian).
9. Zaitsev O.A. Features of the use of electronic information as criminal evidence: A comparative-legal analysis of foreign legislation. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2019, no. 4, pp. 42–57. (In Russian).