УДК 343.14:004 **DOI: 10.34670/AR.2026.89.85.049**

Проблемы признания допустимости и достоверности доказательств в условиях цифровизации

Гонтарь Сергей Николаевич

Кандидат юридических наук, доцент,
Северо-Кавказский федеральный университет,
355000, Российская Федерация, Ставрополь, ул. Пушкина, 1а;
e-mail: gonsernik@gmail.com

Настуев Алан Салихович

Студент,
Северо-Кавказский федеральный университет,
355000, Российская Федерация, Ставрополь, ул. Пушкина, 1а;
e-mail: nastuevvva123@gmail.com

Саиян Борис Арменович

Студент,
Северо-Кавказский федеральный университет,
355000, Российская Федерация, Ставрополь, ул. Пушкина, 1а;
e-mail: estoesai@mail.ru

Данилова Елизавета Витальевна

Студент,
Северо-Кавказский федеральный университет,
355000, Российская Федерация, Ставрополь, ул. Пушкина, 1а;
e-mail: miss.liza230704@yandex.ru

Аннотация

Статья посвящена анализу процесса цифровизации уголовного судопроизводства в Российской Федерации, выявлению правовых и технологических проблем, связанных с обработкой цифровых доказательств, таких как данные из облачных сервисов, социальных сетей и видеозаписи. Авторы показывают, что цифровизация оказывает существенное влияние на сбор, хранение и использование доказательств, что требует внесения изменений в уголовно-процессуальное законодательство для обеспечения соблюдения прав граждан и эффективности расследования. Обоснована необходимость скорейшего урегулирования проблем цифровизации, чтобы обеспечить доверие граждан к цифровому судопроизводству и гарантировать допустимость цифровых доказательств. Предложенные меры обеспечивают баланс между потребностями следствия и правами граждан, создавая надежный правовой режим для работы с цифровыми доказательствами.

Для цитирования в научных исследованиях

Гонтарь С.Н., Настуев А.С., Саиян Б.А., Данилова Е.В. Проблемы признания допустимости и достоверности доказательств в условиях цифровизации // Вопросы российского и международного права. 2026. Том 16. № 1А. С. 397-406. DOI: 10.34670/AR.2026.89.85.049

Ключевые слова

Цифровизация уголовного судопроизводства, электронные доказательства, облачные сервисы, персональные данные, видео-конференц-связь, допустимость доказательств.

Введение

Цифровая трансформация в публичных отраслях права стала одним из ключевых факторов модернизации государственной деятельности. В связи с этим цифровизация уголовного судопроизводства неизбежна, что подтверждает и ряд исследователей, которые говорят о необходимости создания системы цифрового уголовного судопроизводства [Лебедев, Джафарли, 2025, с. 15]. Внедрение информационно-коммуникационных технологий изменяет способы сбора, документирования, проверки и исследования доказательств, а также само организационно-процессуальное выполнение следственных и судебных действий. В Российской Федерации цифровизация уголовного процесса реализуется в виде постепенной интеграции электронного документооборота, использования электронных доказательств, внедрения средств удаленного участия, разработки нормативных механизмов, обеспечивающих правовой режим электронных материалов, доступ к судебной информации и др. На нормативном уровне процесс направлен на совершенствование процессуальных действий, что отражается закреплением соответствующих норм в уголовно-процессуальном законодательстве.

Правовое определение «цифровизации» в уголовном процессе сегодня отсутствует, а его разработка сталкивается с рядом методологических и практических проблем в связи с тем, что цифровизация является технологическим и правовым феноменом. С технологической стороны цифровизация – это внедрение информационных технологий, с правовой – изменение правового режима. В своей повседневной деятельности правоохранительные и судебные органы власти используют информационные технологии, которые согласно ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, представляют процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [Федеральный закон № 149-ФЗ, 2006]. Таким образом, процесс цифровизации состоит из комплекса правовых и технических преобразований, направленных на перевод процессуальных действий, документов, доказательственной деятельности в электронную (цифровую) форму с использованием информационно-коммуникационных технологий при обеспечении процессуальных гарантий сторон и требований к защите информации.

Основная часть

Одной из наиболее сложных сфер цифровизации является обращение с данными, хранящимися в облачных сервисах. Облачные хранилища обладают рядом особенностей. Во-

первых, отсутствует материально выраженный «оригинал» информации: данные существуют как совокупность синхронизированных технических копий в распределённой инфраструктуре. Следователь не может изъять подлинник в традиционном смысле, что усложняет фиксацию доказательств. Во-вторых, данные в облачных сервисах динамичны: автоматические обновления, резервное копирование, синхронизация устройств и алгоритмы оптимизации могут менять содержание файлов без участия человека, что влияет на критерий достоверности. В-третьих, доказательственное значение таких данных напрямую зависит от технических журналов (логов), содержащих информацию о времени доступа, идентификаторах устройств, сеансах и действиях пользователей. В-четвёртых, облачные хранилища часто имеют трансграничный характер, что вызывает необходимость международного взаимодействия и соблюдения законодательства других государств. В-пятых, существует риск удалённого изменения или уничтожения данных пользователем или иным лицом, что повышает вероятность фальсификации цифровых следов. В-шестых, работа с облаками неизбежно связана с обработкой персональных данных, что требует соблюдения гарантий, закреплённых в ст. 23 Конституции РФ [Конституция Российской Федерации, 1993/2020], а также соблюдения требований ст. ст. 164, 164.1 и 183 Уголовно-процессуального кодекса РФ (далее – УПК РФ) [Уголовно-процессуальный кодекс РФ, 2001/2025]. При этом действующее УПК РФ не содержит специальных норм, минимизирующих вмешательство в частную жизнь при доступе к распределённым облачным ресурсам, что создаёт риски несоразмерности вмешательства и угрозу недопустимости доказательств.

Практика подтверждает значимость строгого соблюдения процессуальных требований. Примером служит признание недопустимым доказательства — протокола осмотра облачного хранилища «Мега», составленного с нарушением ст. 66 и 170 УПК РФ, без участия понятых и с признаками фальсификации, при том что само хранилище не было осмотрено в судебном заседании [Кассационное определение Верховного Суда РФ № 2-17/2021, 2023].

В этой связи важно определить порядок правильного составления протокола осмотра облачных данных, предусматривающий обязательное указание технических условий доступа, сведений об используемых средствах фиксации, источников получения данных, временных меток, логов, а также описание последовательности действий следователя. Особое значение имеет участие специалиста, способного обеспечить корректность технических операций и фиксацию метаданных.

Следующей значимой проблемой является признание допустимости и достоверности доказательств, полученных из социальных сетей. Публикации, комментарии, переписка, аудио- и видеоматериалы могут содержать сведения о мотивах, действиях или намерениях участников преступления, однако их использование требует соблюдения процессуальных требований [Гонтарь, О цифровизации..., 2022]. Данные из социальных сетей не названы в УПК РФ как самостоятельный вид доказательств, однако могут выступать «иными документами», если отвечают критериям воспроизводимости, проверки и относимости. Пункт 22 Постановления Пленума ВС РФ № 57 от 26 декабря 2017 г. подтверждает возможность осмотра интернет-страниц, что позволяет использовать распечатки и скриншоты при условии правильной фиксации URL-адреса, времени и источника [Постановление Пленума Верховного Суда РФ № 57, 2017].

Использование данных соцсетей требует законного происхождения доказательств (ст. 75 УПК РФ), подтверждения подлинности и целостности, а также фиксации всех значимых метаданных. Постановление Пленума ВС РФ № 37 от 15 декабря 2022 г. определяет

копирование компьютерной информации как перенос данных на иной носитель или воспроизведение в материальной форме и подчёркивает необходимость соблюдения процедурных гарантий. Важную роль играют технические методы проверки неизменности данных, включая применение электронных подписей, криптографических хеш-сумм и нотариального удостоверения электронных копий. Особое значение имеют компьютерно-техническая и лингвистическая экспертизы, которые позволяют установить авторство, время публикации, происхождение данных, а также оценить стилевые особенности текстов [Постановление Пленума Верховного Суда РФ № 37, 2022].

При этом доступ к личной переписке требует судебного разрешения, в соответствии со ст. 23 Конституции РФ и ст. 13 УПК РФ. Однако Конституционный Суд РФ в Определении от 24 июня 2021 г. № 1364-О указал, что осмотр и экспертиза данных, хранящихся в изъятых устройствах, не требуют отдельного судебного решения, что усложняет баланс интересов следствия и защиты [Определение Конституционного Суда РФ № 1364-О, 2021].

Отдельное направление цифровизации — использование видео-конференц-связи (ВКС) при производстве следственных действий. ВКС является элементом цифровизации, поскольку обеспечивает удалённый доступ, фиксацию действий и передачу данных по защищённым каналам. Однако правовое регулирование в этой сфере пока недостаточно развито. В УПК РФ закреплена ст. 189.1, которая закрепляет, что допрос, очную ставку и опознание можно проводить посредством ВКС. Однако, отсутствуют требования к цифровым платформам, через которые указанные следственные действия можно осуществить [Гонтарь, Отдельные вопросы..., 2023]. Так неясно, допустим ли видеозвонок для проведения допроса, очной ставки и опознания через WhatsApp, MAX или аналогичные мессенджеры. Поскольку наличие такой неясности ставит под угрозу тайну следствия и безопасность данных, то требуется регламентировать перечень цифровых платформ, а также технических средств, которые могут быть использованы при проведении отдельных следственных действий посредством ВКС.

Следует отметить, что технические проблемы (низкая скорость передачи данных, зависание видеосигнала), которые могут возникнуть в результате использования ВКС, способны негативно влиять на качество опознания, допроса или очной ставки и ставить под сомнение допустимость полученных доказательств.

Особенно проблематичным является опознание трупа посредством ВКС. Ст. 189.1 УПК РФ прямо не запрещает такую процедуру, но в условиях, когда труп обезображен и идентификация возможна только по деталям внешности, видеосвязь объективно недостаточна. В таких случаях необходимо личное присутствие опознающего.

Также остаётся открытым вопрос о возможности повторного опознания, если оно было прервано по техническим причинам. При этом ч. 3 ст. 193 УПК РФ запрещает повторное опознание по тем же признакам, что создаёт дополнительную правовую неопределённость.

Особую сложность при работе с цифровыми доказательствами представляет обработка персональных данных, неизбежно возникающая при доступе к информации, размещённой в облачных сервисах, социальных сетях и при использовании видео-конференц-связи. Согласно ст. 23 Конституции РФ, каждому гарантируется право на неприкосновенность частной жизни, личную и семейную тайну, а также тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Эти конституционные гарантии конкретизированы в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), который определяет принципы обработки персональных данных, включая законность, минимизацию и недопустимость объединения баз данных, несовместимых по целям обработки

(ст. 5 № 152-ФЗ) [Федеральный закон № 152-ФЗ, 2006].

Однако действующее уголовно-процессуальное законодательство пока не содержит специальных механизмов, обеспечивающих соблюдение требований законодательства о персональных данных при работе с цифровыми массивами сведений. Так, ст. 164, 164.1 и 183 УПК РФ устанавливают общий порядок выемки, осмотра и копирования электронных данных, но не предусматривают ограничений, направленных на минимизацию вмешательства в частную жизнь при доступе к облачным ресурсам, содержащим большой объём данных, относящихся к частной сфере пользователя. В результате следователь, получая доступ к облачному аккаунту, фактически получает возможность ознакомления с массивами данных, не имеющими отношения к предмету расследования, что противоречит принципу минимизации обработки персональных данных, установленному ст. 5 Закона № 152-ФЗ.

Дополнительную правовую неопределённость создаёт трансграничный характер хранения облачных данных. Нередко персональные данные российских граждан размещаются на серверах иностранных провайдеров, что требует соблюдения требований не только российского законодательства, включая ст. 12 Закона № 152-ФЗ о трансграничной передаче персональных данных, но и законодательства других государств. В отсутствие специальных процедур, предусмотренных УПК РФ, возникает риск признания добытых доказательств недопустимыми по основанию нарушения порядка получения сведений (ст. 75 УПК РФ).

Проблема персональных данных проявляется также при использовании видео-конференц-связи в ходе следственных действий. ВКС предполагает передачу изображения, голоса, поведенческих реакций и иных биометрических идентификаторов, прямо относящихся к специальным категориям персональных данных или к биометрическим персональным данным (ст. 10 и ст. 11 № 152-ФЗ). При этом УПК РФ пока не устанавливает ни требований к уровню защиты используемых цифровых платформ, ни ограничений на применение мессенджеров и иных сервисов, которые не обеспечивают достаточный уровень криптографической защиты и могут быть уязвимы для перехвата или несанкционированного доступа. Отсутствие нормативного перечня допустимых технических средств создаёт угрозу нарушения тайны следствия и прав участников процесса.

Использование информации из социальных сетей и мессенджеров также сопряжено с рисками нарушения режима обработки персональных данных. Социальные сети содержат личную переписку, данные о круге общения, биографические сведения, фото- и видеоматериалы, которые подпадают под правовой режим персональных данных и нередко под специальную категорию данных (биометрические сведения). Доступ к таким данным должен осуществляться только при наличии судебного решения (ст. 23 Конституции РФ, ст. 13 УПК РФ).

Однако процессуальные нормы не устанавливают специальных требований к фиксации метаданных, сохранению целостности цифровых следов и ограничению объёма запрашиваемой информации, вследствие чего существует риск получения избыточных данных, не относящихся к предмету расследования [Гонтарь, Третьяк, 2023].

Обобщая выявленные проблемы цифровизации, можно предложить комплекс мер по совершенствованию уголовно-процессуального регулирования, в частности.

– Следует дополнить ст. 164.1 УПК РФ нормой о создании криптографически удостоверенной зеркальной копии облачных данных с фиксацией хеш-сумм, метаданных и состояния объекта. Важно понимать, что такая копия отличается от обычного копирования: она фиксирует не только пользовательские файлы, но и скрытые

системные данные, подтверждая неизменность содержимого. Кроме того, необходимо установить обязанность провайдера блокировать доступ пользователя к облачному сегменту и сохранять данные в неизменном виде до завершения следственных действий;

– Необходимо нормативно закрепить перечень допустимых технических устройств и определить возможность или запрет использования личных гаджетов следователя или участников процесса при проведении допроса, очной ставки и опознания посредством ВКС;
– Следует дополнить ст. 189.1 УПК РФ нормой о том, что опознание трупа по ВКС допускается только в исключительных случаях — не терпящих отлагательства, при наличии реальной угрозы утраты доказательств;
– Требуется законодательно урегулировать вопрос о возможности повторного опознания, прерванного по техническим причинам, что обеспечит единообразие следственной практики;
– Целесообразно дополнить ст. 164.1 УПК РФ положением, устанавливающим, что при доступе к облачному хранилищу следователь вправе получать только данные, прямо указанные в постановлении о производстве следственного действия, а провайдер облачного сервиса обязан предоставить сведения в форме, исключающей ознакомление с избыточной информацией. Дополнительно следует закрепить обязанность провайдера сформировать криптографически удостоверенную зеркальную копию (клонированный образ) конкретного сегмента данных с фиксацией хеш-сумм и метаданных, что соответствует требованиям ст. 19 Закона № 152-ФЗ о защите персональных данных от неправомерного доступа;
– Предлагается дополнить ст. 183 УПК РФ нормой, предусматривающей обязательное судебное разрешение на изъятие массивов данных, содержащих персональные данные в объёме, превышающем минимально необходимый. Судебное решение должно содержать указание на конкретные категории данных, к которым открывается доступ, и установление запрета на обработку иных сведений;
– С целью защиты прав граждан при проведении следственных действий посредством ВКС следует внести изменения в ст. 189.1 УПК РФ, установив допустимый перечень сертифицированных государством платформ, обеспечивающих защиту биометрических персональных данных с использованием технологий сквозного шифрования (E2EE). Следует прямо запретить использование мессенджеров и иных сервисов, не прошедших государственную сертификацию, что соответствует требованиям ст. 19 Закона № 152-ФЗ о принятии оператором необходимых мер защиты персональных данных;
– В ст. 186.1 УПК РФ необходимо закрепить правило минимизации доступа при истребовании персональных данных из социальных сетей: следователь имеет право получать переписку, сообщения и иные сведения только в пределах, непосредственно относящихся к предмету расследования, а платформа обязана предоставить такие сведения в форме, исключающей получение избыточной информации.

Заключение

Таким образом, цифровизация уголовного судопроизводства в современных условиях выступает не просто направлением технологического развития, но фундаментальным изменением самой природы уголовно-процессуальной деятельности. Она преобразует способы

фиксации, хранения и оценки доказательств расширяет инструменты взаимодействия участников процесса и формирует новые стандарты обеспечения прав граждан. Вместе с тем стремительное внедрение цифровых технологий обнажает ряд правовых противоречий, связанных прежде всего с обращением с облачными данными, информацией из социальных сетей и биометрическими сведениями, обрабатываемыми в рамках видео-конференц-связи. Эти сферы характеризуются повышенным риском вмешательства в личную жизнь, трансграничностью данных, возможностью их удалённого изменения, сложностью подтверждения подлинности и высокой зависимостью от технических условий. Анализ показал, что действующее уголовно-процессуальное законодательство пока не формирует целостного механизма обращения с цифровыми доказательствами, способного одновременно учитывать как интересы эффективного расследования, так и требования законодательства о персональных данных. Отсутствуют нормы, минимизирующие вмешательство в частную жизнь при работе с облачными массивами; не разработаны стандарты фиксации метаданных и проверки целостности информации из социальных сетей; не определены требования к цифровым платформам, используемым для ВКС, что порождает неоднородность практики. Предложенные меры — закрепление обязательного создания криптографически удостоверенных копий облачных данных, введение судебного контроля за доступом к значительным массивам персональной информации, установление перечня сертифицированных платформ для ВКС, формирование правил минимизации доступа к данным из социальных сетей — позволяют сформировать системный, согласованный и технологически адекватный режим работы с цифровыми доказательствами. Их реализация создаёт условия для повышения уровня защищённости персональных данных, укрепления доверия к цифровым процедурам и обеспечения допустимости полученных доказательств. Таким образом, цифровизация уголовного судопроизводства представляет собой неизбежный и объективно необходимый процесс, эффективность которого зависит от способности законодателя своевременно адаптировать процессуальные механизмы к новым технологическим реалиям. Полагаем, что внедрение предложенных изменений позволит добиться баланса между интересами государства в противодействии преступности и конституционными гарантиями прав личности.

Библиография

1. Гонтарь, С. Н. (2022). О цифровизации уголовного судопроизводства. В *Личность, общество, государство в условиях цифровизации: Сборник материалов III Международной научно-практической конференции* (сс. 230-233). Ставрополь: Северо-Кавказский федеральный университет.
2. Гонтарь, С. Н. (2023). Отдельные вопросы проведения допроса с использованием систем видео-конференц-связи. В *Теория и практика расследования преступлений: Материалы XI Международной научно-практической конференции* (сс. 357-358). Краснодар: Краснодарский университет МВД России.
3. Гонтарь, С. Н., & Третьяк, М. И. (2023). Проблемы правовой регламентации и практики реализации норм УПК РФ об охране прав личности в уголовном судопроизводстве. *Гуманитарные и юридические исследования*, 10(3), 453-458.
4. Кассационное определение Верховного Суда Российской Федерации от 15 мая 2023 г. по делу № 2-17/2021. (2023). URL: https://sudact.ru/vsrf/doc/1APFMYRVmPVj/ .
5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). (1993/2020). URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ .
6. Лебедев, С. Я., & Джафарли, В. Ф. (2025). *Цифровое уголовное право*. Москва: Блок-Принт.
7. Определение Конституционного Суда РФ от 24.06.2021 № 1364-О «Об отказе в принятии к рассмотрению жалобы гражданина Фомина Евгения Петровича на нарушение его конституционных прав статьями 93, 176, 177 и частью второй статьи 184 Уголовно-процессуального кодекса Российской Федерации». (2021). URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=674396 .

8. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». (2022). URL: .
9. Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов». (2017). URL: https://www.consultant.ru/document/cons_doc_LAW_286321/ .
10. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 27.10.2025). (2001/2025). URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ .
11. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. (2006). URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ .
12. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. (2006). URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ .

Problems of Recognizing the Admissibility and Reliability of Evidence in the Context of Digitalization

Sergei N. Gontar'

PhD in Law, Associate Professor,
North Caucasus Federal University,
355000, 1a, Pushkina str., Stavropol, Russian Federation;
e-mail: gonsernik@gmail.com

Alan S. Nastuev

Student,
North Caucasus Federal University,
355000, 1a, Pushkina str., Stavropol, Russian Federation;
e-mail: nastuevvva123@gmail.com

Boris A. Saiyan

Student,
North Caucasus Federal University,
355000, 1a, Pushkina str., Stavropol, Russian Federation;
e-mail: estoesai@mail.ru

Elizaveta V. Danilova

Student,
North Caucasus Federal University,
355000, 1a, Pushkina str., Stavropol, Russian Federation;
e-mail: miss.liza230704@yandex.ru

Abstract

The article is devoted to the analysis of the digitalization process of criminal proceedings in the Russian Federation, identifying legal and technological problems associated with the handling of

digital evidence, such as data from cloud services, social networks, and video recordings. The authors show that digitalization has a significant impact on the collection, storage, and use of evidence, which requires amendments to criminal procedure legislation to ensure the protection of citizens' rights and the effectiveness of investigations. The necessity of promptly resolving digitalization problems is substantiated to ensure public trust in digital legal proceedings and guarantee the admissibility of digital evidence. The proposed measures ensure a balance between the needs of the investigation and the rights of citizens, creating a reliable legal regime for working with digital evidence.

For citation

Gontar' S.N., Nastuev A.S., Saiyan B.A., Danilova E.V. (2026) Problemy priznaniya dopustimosti i dostovernosti dokazatel'stv v usloviyakh tsifrovizatsii [Problems of Recognizing the Admissibility and Reliability of Evidence in the Context of Digitalization]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (1A), pp. 397-406. DOI: 10.34670/AR.2026.89.85.049

Keywords

Digitalization of criminal proceedings, electronic evidence, cloud services, personal data, video conferencing, admissibility of evidence.

References

1. Federalnyy zakon "O personalnykh dannykh" ot 27.07.2006 № 152-FZ [Federal Law "On Personal Data" No. 152-FZ of July 27, 2006]. (2006). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_61801/
2. Federalnyy zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" ot 27.07.2006 № 149-FZ [Federal Law "On Information, Information Technologies and Information Protection" No. 149-FZ of July 27, 2006]. (2006). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_61798/
3. Gontar', S. N. (2022). O tsifrovizatsii ugolovnogo sudoproizvodstva [On digitalization of criminal proceedings]. In *Lichnost, obshchestvo, gosudarstvo v usloviyakh tsifrovizatsii: Sbornik materialov III Mezhdunarodnoy nauchno-prakticheskoy konferentsii* (pp. 230-233). Stavropol: Severo-Kavkazskiy federalnyy universitet.
4. Gontar', S. N. (2023). Otdelnyye voprosy provedeniya doprosa s ispolzovaniyem sistem video-konferents-svyazi [Selected issues of interrogation using video conferencing systems]. In *Teoriya i praktika rassledovaniya prestupleniy: Materialy XI Mezhdunarodnoy nauchno-prakticheskoy konferentsii* (pp. 357-358). Krasnodar: Krasnodarskiy universitet MVD Rossii.
5. Gontar', S. N., & Tretyak, M. I. (2023). Problemy pravovoy reglamentatsii i praktiki realizatsii norm UPK RF ob okhrane prav lichnosti v ugolovnom sudoproizvodstve [Problems of legal regulation and practice of implementing the norms of the Code of Criminal Procedure of the Russian Federation on the protection of individual rights in criminal proceedings]. *Gumanitarnyye i yuridicheskiye issledovaniya*, 10(3), 453-458.
6. Kasatsionnoye opredeleniye Verkhovnogo Suda Rossiyskoy Federatsii ot 15 maya 2023 g. po delu № 2-17/2021 [Cassation Ruling of the Supreme Court of the Russian Federation of May 15, 2023 in case No. 2-17/2021]. (2023). Retrieved from https://sudact.ru/vsrf/doc/1APFMYRVmPVj/
7. Konstitutsiya Rossiyskoy Federatsii (prinyata vsenarodnym golosovaniyem 12.12.1993 s izmeneniyami, odobrennymi v khode obshcherossiyskogo golosovaniya 01.07.2020) [The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993, with amendments approved during the all-Russian vote on 01.07.2020)]. (1993/2020). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_28399/
8. Lebedev, S. Ya., & Dzhafarli, V. F. (2025). *Tsifrovoye ugolovnoye pravo* [Digital Criminal Law]. Moscow: Blok-Print.
9. Opredeleniye Konstitutsionnogo Suda RF ot 24.06.2021 № 1364-O "Ob otkaze v prinyatii k rassmotreniyu zhaloby grazhdanina Fomina Yevgeniya Petrovicha na narusheniye yego konstitutsionnykh prav statyami 93, 176, 177 i chastyu vtoroy stati 184 Ugolovno-protsessualnogo kodeksa Rossiyskoy Federatsii" [Ruling of the Constitutional Court of the Russian Federation No. 1364-O of June 24, 2021 "On the refusal to accept for consideration the complaint of citizen Evgeny Petrovich Fomin about the violation of his constitutional rights by Articles 93, 176, 177 and part two of Article 184 of the Code of Criminal Procedure of the Russian Federation"]. (2021). Retrieved from https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=674396

10. Postanovleniye Plenuma Verkhovnogo Suda RF ot 15.12.2022 № 37 "O nekotorykh voprosakh sudebnoy praktiki po ugolovnym delam o prestupleniyakh v sfere kompyuternoy informatsii, a takzhe inykh prestupleniyakh, sovershennykh s ispolzovaniyem elektronnykh ili informatsionno-telekommunikatsionnykh setey, vklyuchaya set 'Internet'" [Resolution of the Plenum of the Supreme Court of the Russian Federation No. 37 of December 15, 2022 "On some issues of judicial practice in criminal cases on crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet"]. (2022). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_434573/
11. Postanovleniye Plenuma Verkhovnogo Suda RF ot 26.12.2017 № 57 "O nekotorykh voprosakh primeneniya zakonodatelstva, reguliruyushchego ispolzovaniye dokumentov v elektronnom vide v deyatelnosti sudov obshchey yurisdiktsii i arbitrazhnykh sudov" [Resolution of the Plenum of the Supreme Court of the Russian Federation No. 57 of December 26, 2017 "On some issues of applying legislation regulating the use of electronic documents in the activities of courts of general jurisdiction and arbitration courts"]. (2017). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_286321/
12. Ugolovno-protsessualnyy kodeks Rossiyskoy Federatsii ot 18.12.2001 № 174-FZ (red. ot 27.10.2025) [Code of Criminal Procedure of the Russian Federation No. 174-FZ of December 18, 2001 (as amended on October 27, 2025)]. (2001/2025). Retrieved from https://www.consultant.ru/document/cons_doc_LAW_34481/