Дата поступления рукописи в редакцию: 04.10.2026 г. DOI: 10.24412/2224-9133-2026-10-583-589
Дата принятия рукописи в печать: 10.11.2026 г.

ШЕСТАК Виктор Анатольевич,
доктор юридических наук, доцент, профессор кафедры криминалистики Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева,
e-mail: viktor_shestak@mail.ru

О ПРОБЛЕМНЫХ АСПЕКТАХ ИНСТИТУТА ВЕЩЕСТВЕННЫХ ЭЛЕКТРОННЫХ (ЦИФРОВЫХ) ДОКАЗАТЕЛЬСТВ

Аннотация. *Статья посвящена доктринальному и законодательному анализу института вещественных доказательств в уголовном судопроизводстве. Автор исследует эволюцию понятия вещественных доказательств — от классических материальных носителей до цифровых данных. Особое внимание уделено проблеме электронных (цифровых) вещественных доказательств, правовой статус которых до сих пор не получил системного закрепления в российском праве. Автор затрагивает вопросы процессуальной фиксации цифровых данных, их аутентичности, целостности и криптографического хеширования, обращаясь к отечественному и международному опыту. Автор приходит к выводу о наличии теоретических разногласий и отсутствии единообразия в правоприменительной практике при работе с электронными (цифровыми) доказательствами. Анализируя тенденции развития понятия «электронного доказательства», автор отмечает отсутствие четкого представления и единого мнения о сущности доказательств в электронной форме на данном этапе развития уголовно-процессуального законодательства в России, что приводит к теоретическим разногласиям и отсутствию единообразия в правоприменительной практике при обращении с ними.*

Ключевые слова: *вещественные доказательства, электронные доказательства, доказывание, цифровизация уголовного процесса, криптографическое хеширование.*

Для цитирования: *Шестак В. А. О проблемных аспектах института вещественных электронных (цифровых) доказательств // Право и управление. 2026. № 10. С. 583–589.*

SHESTAK V.A.,
Doctor of Juridical Science, Associate Professor, Professor of the Department of Criminalistics, A.Ya. Sukharev Moscow Academy of the Investigative Committee of the Russian Federation

ON THE PROBLEMATIC ASPECTS OF THE INSTITUTE OF EVIDENTIAL ELECTRONIC (DIGITAL) EVIDENCE

Annotation. *The article is devoted to a doctrinal and legislative analysis of the institution of physical evidence in criminal proceedings. The author examines the evolution of the concept of physical evidence — from classical material carriers to digital data. Special attention is paid to the problem of electronic (digital) physical evidence, the legal status of which has not yet been systematically established in Russian law. The author addresses issues related to the procedural recording of digital data, their authenticity, integrity, and cryptographic hashing, drawing on domestic and international experience. The author concludes that there are theoretical disagreements and a lack of uniformity in law enforcement practice when dealing with electronic (digital) evidence. Analyzing the trends in the development of the concept of «electronic evidence». The author notes the absence of a clear understanding and a unified view on the essence of evidence in electronic form at this stage of the development of criminal procedure legislation in Russia, which leads to theoretical disagreements and a lack of uniformity in law enforcement practice when dealing with such evidence.*

Key words: *physical evidence, electronic evidence, proof, digitalization of criminal proceedings, cryptographic hashing.*

For citation: *Shestak V. A. On the problematic aspects of the institute of evidential electronic (digital) evidence. Law and administration. 2026;(10):583–589. (In Russ.).*

Институт вещественных доказательств занимает центральное положение в системе доказательственного права, выступая материальным носителем криминалистически значимой информации о событии правонарушения. В условиях стремительной цифровизации общественных отношений и технологической трансформации преступности традиционные процессуальные конструкции, сформированные для работы с физическими объектами, демонстрируют недостаточную адаптивность к новым реалиям. Это порождает комплекс теоретических и практических проблем, связанных с собиранием, процессуальным закреплением, экспертным исследованием и оценкой вещественных доказательств, особенно в их электронной (цифровой) форме.

Понятие вещественных доказательств в юридической науке и законодательстве формировалось как ответ на необходимость объективизации процесса доказывания, обеспечивая материальную основу для установления истины по делу. В процессуальной доктрине вещественные доказательства традиционно рассматриваются как материальные объекты, которые в силу своих физических свойств, местоположения, внешних признаков или содержащейся информации способны подтвердить или опровергнуть обстоятельства, имеющие значение для разрешения дела. Такие исследователи как А.Р. Белкин [1] и М. К. Треушников [2], считают, что ключевой характеристикой вещественных доказательств является их способность сохранять «немые следы» события — отпечатки пальцев на орудии преступления, повреждения на одежде потерпевшего, записи камер наблюдения или электронные следы в виде метаданных. Доктрина акцентирует двойственную природу таких доказательств: с одной стороны, их объективность как материальных носителей информации, с другой — субъективность интерпретации, поскольку значимость предмета определяется через его связь с событием, устанавливаемую участниками процесса. К примеру, найденный нож становится доказательством только после подтверждения его принадлежности обвиняемому и наличия на нем биологических следов жертвы.

М. С. Строгович, в свою очередь, определял вещественные доказательства как «любую вещь, которая в соответствии с установленными процессуальным законом условиями может служить доказательством по делу, то есть быть источником по делу о доказательственном и главном факте и тем самым устанавливать существенные для дела обстоятельства» [3]. А А.Я. Вышинский полагал вещественное доказательство предметом, служащим уликой совершенного преступления, уликой, изобличающей лицо, совершившее преступление, или служащее для его оправдания, для установления, в частности, его алиби [4].

Законодательное закрепление понятия вещественных доказательств в российском праве содержится в нормах ст. 81 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) [5] и ст. 73 Гражданского процессуального кодекса Российской Федерации (далее – ГПК РФ) [6]. Так, согласно ч. 1 ст. 81 УПК РФ, вещественными доказательствами признаются любые предметы, которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления; на которые были направлены преступные действия; деньги, ценности и иное имущество, полученные в результате совершения преступления; иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела. ГПК РФ расширяет трактовку, включая любые материальные объекты, которые могут быть использованы для установления обстоятельств гражданского дела.

Законодатель акцентирует процессуальную форму работы с такими доказательствами: изъятие должно сопровождаться составлением протокола с участием понятых, описание должно быть детализированным, а хранение — обеспечивать сохранность до окончания производства по делу. Однако легальные дефиниции не всегда успевают за технологическими изменениями: цифровые носители информации (электронные письма, данные блокчейна, логи серверов) формально подпадают под категорию вещественных доказательств, но специфика их изъятия, фиксации и исследования требует особых норм, которые в российском праве до сих пор не систематизированы. В этой связи, полагаем, что вещественные доказательства допустимо рассматривать как материальные объекты (предметы, вещества, следы), которые обладают признаками, позволяющими установить обстоятельства, имеющие значение для дела.

Исследователи не зря обращают внимание на трудности постижения, восприятия и оценки природы вещественных доказательств, аргументируя свое мнение тем, что в отличие от личных

доказательств, являющихся по своему содержанию «обычными» и «очевидными», последние отличает многообразие их форм и видов. Одним из таких противоречивых представителей, который, к сожалению, по сей день не нашел своего официального закрепления в процессуальном законодательстве России, является институт «электронных (цифровых) доказательств». Будучи всеобъемлющим хранилищем колоссального объема информации, способным предоставить ее для практического применения, используя в обязательном порядке соответствующий материальный носитель, теоретическое и практическое применение такого феномена предполагает необходимость законодательных новелл.

В эпоху цифровых технологий и глобализации преступности вещественные доказательства становятся как более значимыми, так и более уязвимыми. Их роль усиливается в делах, связанных с киберпреступлениями, экономическими мошенничествами и терроризмом, где материальные следы часто носят скрытый или технически сложный характер. Это подтверждается статистическими данными МВД России [7], демонстрирующими порой разнонаправленную динамику. Так, в четвёртом квартале 2024 года общий уровень криминальной активности в стране демонстрировал положительную динамику: количество зафиксированных правонарушений сократилось на 1,8% по сравнению с аналогичным периодом предыдущего года. Однако структурный анализ преступности выявляет тревожную тенденцию: две пятых всех инкриминируемых деяний (40%) были реализованы с применением цифровых технологий и интернет-коммуникаций. Углублённое изучение показателей свидетельствует о резкой эскалации киберпреступности. Число таких инцидентов превысило значения 2023 года на 13,1%, причём наиболее опасные категории – тяжкие и особо тяжкие составы – увеличились на 7,8%. Именно эта группа правонарушений стала драйвером роста общефедерального показателя по особо опасным преступлениям, который в годовом исчислении поднялся на 4,8%.

По итогам 2025 года количество зарегистрированных киберпреступлений составило приблизительно 650 тысяч, что отражает снижение по сравнению с 2024 годом, когда было зафиксировано около 765,5 тысяч таких преступлений. За первые пять месяцев 2026 года число преступлений, совершённых с использованием информационно-телекоммуникационных технологий, сократилось на 31,2% по сравнению с аналогичным периодом 2025 года; при этом преступления в сфере компьютерной информации снизились на 38,7%, дистанционные кражи — на 17,8%, IT-мошенничество — на 26,4%. В результате принятия Правительством Российской Федерации в 2025–2026 годах ряда законодательных пакетов (в частности таких, как: «Антифрод 1.0» и «Антифрод 2.0»), направленных на противодействие кибермошенничеству, за первые семь месяцев 2026 года ущерб от кибермошенничества снизился на 21% по сравнению с аналогичным периодом 2025 года.

В современных судопроизводствах, в том числе и в уголовном, все чаще фигурируют электронные (цифровые) данные, которые активно применяются как доказательство в рассматриваемых делах. Так, по мнению Р.И. Оконенко, цифровая информация обладает следующим рядом юридически важных свойств: носители электронной информации способны хранить значительный объем электронных сведений; легкость копирования информации, содержащейся на электронном носителе, без ее деформирования; уязвимость электронных сведений в части простоты их изменения и уничтожения; возможность хранения информации как в памяти устройств, так и в Интернете или иной информационно-телекоммуникационной системе; латентность некоторой части информации, которая доступна лишь лицам, обладающим специальными знаниями в области компьютерной информации. К таким сведениям относятся метаданные, содержащие важную информацию об операциях пользователя [8].

Однако отметим, что наравне с этим растут и риски фальсификации, утраты или повреждения доказательств из-за недостатков в законодательном регулировании и практических механизмах работы с ними. Кроме того, их использование в процессах сопряжено с рядом особенностей и трудностей, - от проблем понимания их природы до проблем процессуального обеспечения. К примеру, в российском уголовно-процессуальном законодательстве электронные доказательства не выделены как самостоятельная категория; они рассматриваются в рамках норм ст.ст. 74, 81 и 84 УПК РФ, что создаёт правовую неопределённость в отношении их допустимости, подлинности и порядка представления. Говоря о природе электронных (цифровых) доказательств, полагаем, следует отталкиваться от синонимически схожего понятия информации, которое закреплено в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [9], где под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Согласно Постановлению Пленума Верховного Суда Российской Федерации 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-телеком-

муникационных сетей, включая сеть "Интернет"» [10] использование цифровой информации в уголовно-процессуальном доказывания сопряжено с обязательным подробным анализом представленных сведений специалистами в данной отрасли. В этой связи, полагаем, что основной особенностью электронной информации является ее восприятие только с помощью специальных технических устройств. Отсюда следует, что электронная информация представляет собой значимые для расследования преступления сведения, представленные в цифровом формате, воспроизведение которых невозможно без применения технических средств.

Согласно действующему законодательству, данные на электронных носителях могут быть извлечены через проведение следственных действий: осмотра места происшествия, осмотров предметов и документов, обыска, выемки, личного обыска, осмотра и выемки почтово-телеграфной корреспонденции. Норма, предусмотренная ст. 164.1 УПК РФ, устанавливает ограничения при изъятии цифровых устройств хранения данных в ходе расследований, связанных с предпринимательской деятельностью: изъятие допускается лишь при наличии постановления о назначении экспертизы, судебного решения, при отсутствии у владельца законных полномочий на хранение информации, при риске совершения новых преступлений или при невозможности копирования без изменения данных. При этом ключевой проблемой остаётся процессуальная фиксация цифровых доказательств. Традиционные нормы, требующие составления протокола изъятия с участием понятых, предполагают физическое присутствие носителя информации, что невозможно при работе с облачными сервисами. Правоприменитель сталкивается с парадоксом: данные, имеющие критическое значение для дела, формально не могут быть изъяты в соответствии с процессуальными нормами, поскольку отсутствует материальный объект для опечатывания и приобщения к материалам дела. Это приводит к тому, что правоприменители прибегают к альтернативным методам: созданию скриншотов или копированию файлов, которые суды нередко отклоняют из-за отсутствия гарантий целостности и аутентичности.

Техническая сложность, к тому же, усугубляется эфемерностью цифровых доказательств: они могут быть изменены, удалены или перемещены в любой момент. Сообщения в мессенджерах могут автоматически удаляться, данные в облачных хранилищах – синхронизироваться между устройствами, оставляя следы на серверах в разных юрисдикциях. Попытки зафиксировать такие данные через скриншоты лишают их метаданных (время создания, IP-адреса, геолокация) и делают уязвимыми для манипуляций. Сложности здесь начинаются уже на этапе определения юрисдикции над цифровыми доказательствами. Сообщение в мессенджере, отправленное через сервер, расположенный в другом регионе, или данные, хранящиеся в распределенной блокчейн-сети, ставят вопрос о правомочности их изъятия. Законодательство, как правило, отстает от технологических реалий: нормы, регулирующие изъятие содержания электронных писем, могут не учитывать особенности децентрализованных систем хранения. Как следствие - правоприменитель вынужден опираться на аналогии права (закона) или конкретные судебные решения, что повышает риски процессуальных нарушений. В частности, в практике российских судов неоднозначно трактуется статус скриншота переписки из социальной сети: некоторые инстанции признают его допустимым доказательством при наличии подтверждения подлинности, другие требуют проведения экспертизы устройства, с которого была сделана запись.

Технические аспекты работы с вещественными электронными (цифровыми) доказательствами, в свою очередь, усугубляются стремительным развитием технологий шифрования и методов противодействия криминалистическому анализу. Приложения с end-to-end шифрованием, такие как Telegram или Signal, делают невозможным доступ к содержимому переписки без физического обладанием устройства и знания пароля. К примеру, расследуя уголовное дело, даже при успешном изъятии смартфона следователи сталкиваются с проблемой взлома современных моделей, защищенных биометрической аутентификацией и аппаратными модулями безопасности. В таких условиях критически важной становится роль специалистов по компьютерной криминалистике, чья квалификация должна охватывать не только знание программное обеспечение для восстановления данных, но и понимание архитектуры процессоров или особенностей файловых систем.

Полагаем, что ключевым инструментом обеспечения целостности Электронных (цифровых) доказательств является криптографическое хеширование: процесс преобразования данных в уникальную строку символов (хеш), которая изменяется при любой модификации файла. В правовом контексте это позволяет утверждать, что доказательство не подвергалось изменениям с момента изъятия. Однако российское законодательство не содержит прямых требований к использованию хеширования, что приводит к противоречивой практике. При этом современный международный опыт демонстрирует более системный подход. Так, в США Федеральные правила доказательств (FRE) требуют, чтобы электрон-

ные доказательства сопровождались метаданными и хеш-суммами (Правило 902(14)) [11]. В ЕС Регламент eIDAS устанавливает стандарты для электронных подписей и штампов времени [12], что позволяет отслеживать цепочку (custody – англ. – прим. автора) цифровых данных.

Вместе с тем вопрос процессуального регламентирования понятия и классификации доказательств в электронной (цифровой) форме остается открытым, что влечет за собой плодотворную почву для дискуссий. Множество отечественных и зарубежных авторов посвятили свои работы проблемам правового закрепления статуса электронных доказательств. Вместе с тем согласно нормам УПК РФ, информация в электронной форме может выступать в качестве вещественных доказательств или иных документов. Классификация данного вида доказательств возможна по различным основаниям, в том числе, исходя из формы преставления электронной информации, ее свойств, носителей, а также структурного содержания. Собирание, проверка и оценка электронных (цифровых) доказательств с одной стороны подчиняется общим правилам, присущим любым видам доказательств, а с другой стороны имеет особенности, связанные со спецификой объектов цифровой информации. Так, для признания допустимыми доказательств в электронной форме, следователю необходимо соблюдать процедуру собирания доказательств, опираясь на специальные знания о природе такого рода информации, а в случае необходимости использовать специальные технические средства и привлекать для участия специалиста.

Кроме того, в России, полагаем, наметились существенные подвижки правового регулирования в рассматриваемой сфере. Так, Федеральный закон от 20.02.2026 № 38-ФЗ ввёл новую норму, предусматривающую имплементацию ст. 164.2 УПК РФ, детально регулирующую изъятие цифровых активов (криптовалют) по делам об отмывании доходов, уклонении от уплаты налогов и иным составам; а сама криптовалюта официально признана имуществом в уголовном процессе. Помимо этого, Верховный Суд Российской Федерации в своих разъяснениях от 25.03.2026 подтвердил, что переписка в Telegram и WhatsApp, аудиосообщения и иные цифровые коммуникации признаются полноценными доказательствами при надлежащей идентификации участников и правильной фиксации. А в научной юридической литературе уже обосновывается целесообразность закрепления цифровых доказательств в как самостоятельного вида – в норме ст. 74 УПК РФ, а также включения определения электронных доказательств в норму ст. 5 УПК РФ.

Таким образом, во-первых, снижение количественных показателей киберпреступности при росте стоимостного ущерба свидетельствует о качественной трансформации киберпреступности в сторону более сложных, технически оснащённых схем. Статистические сведения МВД России свидетельствуют, что за первые пять месяцев 2026 года число IT-преступлений сократилось на 31,2%, однако объём похищенных средств в 2025 году достиг 29,3 млрд рублей — на 6,4% больше, чем в 2024 году, что, полагаем, создаёт парадоксальную ситуацию: при формальном снижении преступности потребность в совершенствовании методов работы с электронными (цифровыми) доказательствами не только не уменьшается, но возрастает, поскольку оставшиеся схемы отличаются большей технической изощрённостью и требуют более сложной процессуальной фиксации. Во-вторых, принятие ст. 164.2 УПК РФ (регулирование изъятия криптовалют) и разъяснений Верховного Суда Российской Федерации от 25.03.2026 о признании цифровой переписки доказательством формирует предпосылки для законодательного закрепления электронных (цифровых) доказательств как самостоятельной категории. Однако, фрагментарный характер этих новелл, т.е., по сути, регулирование отдельных аспектов без системной дефиниции, сохраняет риск правоприменительных ошибок и противоречивой судебной практики, что, по-нашему мнению, требует комплексной доработки норм, предусмотренных ст.ст. 5 и 74 УПК РФ. В-третьих, отсутствие в российском законодательстве обязательного требования к криптографическому хешированию при изъятии цифровых доказательств создаёт системную уязвимость доказательственной базы, поскольку современный международный опыт свидетельствует, что хеш-суммы и метаданные являются минимальным стандартом обеспечения целостности. Внедрение подобных требований в нормы УПК РФ позволило бы, по-нашему мнению, существенно снизить долю доказательств, признаваемых недопустимыми по мотиву неподтверждённой аутентичности. В-четвертых, принципиальные запреты на изменение метаданных и подключение посторонних носителей, установленные судебной практикой в период 2024-2026 гг., фактически формируют новый стандарт недопустимости для цифровых доказательств в России. Любое отступление от этого стандарта: ненадлежащая фиксация транзакционных данных, отсутствие квалифицированного специалиста при изъятии и проч. становится самостоятельным основанием для оспаривания доказательственного значения изъятого. А значит: судебная практика опережает законодательство в формировании процессуальных требований к вещественным электронным (цифровым) доказательствам, что усиливает аргументацию в пользу скорейшего нормативного

закрепления.

Список литературы:

[1] Белкин, А. Р. Теория доказывания в уголовном судопроизводстве : учебник для вузов / А. Р. Белкин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. 471 с.

[2] Треушников, М. К. Судебные доказательства / М. К. Треушников. – 5-е изд., доп. – М. : Городец, 2017. – 302 с.

[3] Строгович М.С. Уголовный процесс. – М.: Юрид. изд-во министерства юстиции СССР, 1946.

[4] Вышинский А.Я. Теория доказательств в советском праве. – М., 1941. 294 с.

[5] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2026). – Электронный ресурс. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699 (дата обращения: 30.09.2026).

[6] Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 04.08.2026) (с изм. и доп., вступ. в силу с 01.09.2026). – Электронный ресурс. – URL: https://www.consultant.ru/document/cons_doc_LAW_39570 (дата обращения: 30.09.2026).

[7] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2024 года. МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328 (Дата обращения 30.09.2026).

[8] Окоменко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3. С. 120-124.

[9] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Электронный ресурс. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 30.09.2026).

[10] 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"». – Электронный ресурс. – URL: https://www.consultant.ru/document/cons_doc_LAW_434573 (дата обращения: 30.09.2026).

[11] Federal rules of evidence. U.S. government publishing office. Washington : 2021 – электронный ресурс. – Электронный ресурс. – URL: https://www.wipo.int/wipolex/ru/legislation/details/23158 (дата обращения: 30.09.2026).

[12] Regulation (EU) no 910/2014 of the European parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. – Электронный ресурс. – URL: https://www.legislation.gov.uk/eur/2014/910 (дата обращения: 30.09.2026).

References:

[1] Belkin, A. R. Theory of evidence in criminal proceedings: a textbook for universities / A. R. Belkin. - 2nd ed., Rev. and add. - Moscow: Yurayt Publishing House, 2025. 471 s.

[2] Treushnikov, M.K. Forensic evidence / M.K. Treushnikov. - 5th ed., Add. - M.: Gorodets, 2017. - 302 s.

[3] Strogovich M.S. Criminal trial. - M.: Jurid. Publishing House of the Ministry of Justice of the USSR, 1946.

[4] Vyshinsky A.Ya. Theory of evidence in Soviet law. - M., 1941. 294 pp.

[5] Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended 04.08.2026). - Electronic resource. - URL: https://www.consultant.ru/document/cons_doc_LAW_10699 (access date: 30.09.2026).

[6] Civil Procedure Code of the Russian Federation of 14.11.2002 No. 138-FZ (as amended 04.08.2026) (with amendments and additions, entry by virtue of 01.09.2026). - Electronic resource. - URL: https://www.consultant.ru/document/cons_doc_LAW_39570 (access date: 30.09.2026).

[7] Brief description of the state of crime in the Russian Federation for January - December 2024. Ministry of Internal Affairs of Russia. URL: https ://xn--b1aew.xn--p1ai/reports/item/60248328 (Date accessed 30.09.2026).

[8] Okonenko R.I. Electronic evidence as a new direction of improvement of Russian criminal procedure law // Actual problems of Russian law. 2015. № 3. S. 120-124.

[9] Federal Law No. 27.07.2006 of 149-FZ "On Information, Information Technologies and Information Protection." Electronic resource. - URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (access date: 30.09.2026).

[10] Resolution of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 No. 37 "On certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet." - Electronic resource. - URL: https://www.consultant.ru/document/cons_doc_LAW_434573 (access date: 30.09.2026).

[11] Federal rules of evidence. U.S. government publishing office. Washington: 2021 - electronic resource. - Electronic resource. - URL: https://www.wipo.int/wipolex/ru/legislation/details/23158 (access

date: 30.09.2026).

[12] Regulation (EU) no 910/2014 of the European parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. - Electronic resource. - URL: https://www.legislation.gov.uk/eur/2014/910 (access date: 30.09.2026).

