Научная статья
https://doi.org/10.24412/2220-2404-2025-12-46
УДК 347

ЮРИДИЧЕСКИЕ КРИТЕРИИ ДОВЕРИЯ В СФЕРЕ ЭЛЕКТРОННОЙ ПОДПИСИ: ПРАВОВЫЕ ПРИНЦИПЫ И ТРЕБОВАНИЯ, ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ

Соловяненко Н.И.
Институт государства и права Российской академии наук

Аннотация. *Информационно-коммуникационных технологии, которые лежат в основе цифровой экономики, позволяют физическим и юридическим лицам быстро и эффективно взаимодействовать в условиях цифровизации. Целью данного исследования является анализ юридических конструкций, при помощи которых достигается доверие участников к экономической и социальной деятельности в цифровой среде, определенность в отношении подтверждения личности, правомерности, юридической силы и последствий онлайн операций. Методология исследования основана на анализе российского и зарубежного законодательства и проблем правоприменения с использованием системно-структурного, юридико-догматического и сравнительно-правового методов. Результаты показывают, что юридический механизм электронных подписей базирующийся на технологических и юридических принципах и условиях, обеспечивает пользователям необходимый уровень надежности цифрового взаимодействия. К юридическим критериям доверия квалифицированной электронной подписи принадлежат строгие требования законодательства к аккредитованному удостоверяющему центру, машиночитаемой доверенности, ответственности, а также федеральный государственный контроль. Сделаны выводы о направлениях совершенствовании законодательства в целях укрепления доверия к цифровому взаимодействию с применением электронных подписей: определить понятие «доверенное взаимодействие», урегулировать механизм длительного архивного хранения документов с электронной подписью и ряд других.*

Ключевые слова: *электронная подпись, юридическая значимость, квалифицированная электронная подпись, аккредитованный удостоверяющий центр, квалифицированный сертификат ключа проверки электронной подписи, машиночитаемая доверенность, федеральный государственный контроль (надзор) в сфере электронной подписи, ответственность аккредитованного удостоверяющего центра.*

Финансирование: *инициативная работа.*

Original article

LEGAL CRITERIA OF TRUST IN THE FIELD OF ELECTRONIC SIGNATURE: LEGAL PRINCIPLES AND REQUIREMENTS, FEDERAL STATE CONTROL

Nina I. Solovyanenko
Institute of State and Law of the Russian Academy of Sciences

Abstract*. Information and communication technologies, which underlie the digital economy, allow individuals and legal entities to interact quickly and effectively in the context of digitalization. The purpose of this study is to analyze the legal structures by which participants' trust in economic and social activities in the digital environment is achieved, as well as certainty regarding identity verification, legality, legal force, and the consequences of online transactions. The research methodology is based on an analysis of the Russian and foreign legislative framework and the problems of law enforcement using system-structural, legal-dogmatic and comparative legal methods. The results show that the legal mechanism of electronic signatures, based on technological and legal principles and conditions, provides users with the necessary level of reliability of digital interaction. The legal criteria for trusting a qualified electronic signature include strict legal requirements for an accredited certification center, a machine-readable power of attorney, responsibility, and federal state control. Conclusions are drawn about the directions of improving legislation in order to strengthen trust in digital interaction using electronic signatures: to define the concept of "trusted interaction", to regulate the mechanism of long-term archival storage of documents with electronic signatures, and a number of others.*

Keywords: *electronic signature, legal significance, qualified electronic signature, accredited certification center, qualified electronic signature verification key certificate, machine-readable power of attorney federal state control (supervision) in the field of electronic signature, responsibility of an accredited certification center.*

Funding: *Independent work.*

Введение. В современном мире физические и юридические лица осуществляют доступ к цифровым платформам и услугам в режиме онлайн благодаря применению информационно-коммуникационных технологий, которые лежат в основе цифровой экономики, что позволяет быстро, эффективно и безопасно взаимодействовать с государственными органами и

организациями частного сектора [1, с.93; 2, с.37-41], совершать сделки и иные юридические действия[3, с.36], обращаться за получением государственных и муниципальных услуг, участвовать в процедурах защиты прав и законных интересов, осуществлять культурную, благотворительную и волонтерскую деятельность [4, с.28-35; 5, с.23-38].

Инновационные цифровые технологии, стимулируют устойчивый экономический рост, позволяют максимально использовать удалённую работу и аутсорсинг на различных облачных платформах. Технологические решения улучшают доступность государственных и муниципальных услуг, включая социальное обслуживание, непосредственно влияющих на улучшение качества жизни населения [6, с.66-67]. Применение цифровых технологий судебной системой и нотариатом способствуют доступности институтов защиты прав. Так, цифровой документооборот в суде начиная с подачи исковых заявлений и заканчивая выдачей исполнительных листов и возможность участвовать в судебном процессе удаленно, позволяют экономить время и сокращать финансовые затраты [7, с.391-395]. Вместе с тем использование цифрового формата предполагает применение специальных юридических конструкций. При помощи последних достигается определенность в отношении правомерности, юридической силы и последствий совершаемых дистанционно операций, допустимости качестве доказательств. Не имея подобной определенности невозможно установить доверие участников и общества в целом к результатам экономической и социальной деятельности в цифровой среде.

Обсуждение. Для правового признания цифровых электронных/цифровых операций органами публичной власти или частными лицами необходимо посредством соответствующих юридических конструкций и процедур подтвердить правосубъектность действующих удаленно физических и юридических лиц, а также установить происхождение, подлинность и целостность цифровых документов на всех этапах их жизненного цикла от создания и передачи до электронного архивирования.

Юридическим механизмом, обеспечивающим подтверждение личности, юридической значимости, действительности, а также правовые последствия операций в цифровой среде, является применение при осуществлении данных операций электронной подписи. Интегрированная в процедуры онлайн-взаимодействия и документооборота электронная подпись дает возможность определить подписывающее лицо, проверить подлинность электронных документов и гарантировать их целостность. Виды электронных подписей (простая, усиленная неквалифицированная, усиленная квалифицированная) а также их технологическая, организационная и юридическая инфраструктура предусмотрены в законодательстве РФ. Федеральный закон от 6.04.2011 г. N 63-ФЗ «Об электронной подписи» закрепил централизованный институциональный механизм, включающий субъектов и оказываемые ими «доверенные услуги» (доверенные сервисы) в цифровой среде [8, с.118-119]. Последние могут включать создание электронной подписи, проставление электронную метку времени, выдачу сертификатов ключей проверки электронных подписей и ряд других К числу субъектов принадлежат в том числе удостоверяющие центры (аккредитованные удостоверяющие центры), доверенные лица удостоверяющих центров, доверенные третьи стороны.

Правовое регулирование и применение электронных подписей в различных юрисдикциях базируется на технологических и юридических принципах и критериях надежности цифрового взаимодействия, которое они обеспечивают и соответственно, доверии к такому взаимодействию. Так, например, необходимо подтверждение личности сторон с целью совершении ими дистанционных сделок, в том числе при подписании договора, для выражения согласия с его содержанием. Процедура подписания непосредственно связана с определением воли субъекта, совершающего юридические действия. В этой связи необходимо согласиться с тем, что «выяснение воли человека – главное в действиях нотариуса» [9, с.3]. Часто требуется, чтобы участники электронного взаимодействия производили обмен юридически значимыми документами по надежным, защищенным каналам. Например, Единая информационная система нотариата (ЕИС) является платформой электронного делопроизводства и документооборота в нотариальной деятельности с использованием квалифицированной электронной подписи.

Электронные подписи должны соответствовать системе юридических и технологических требований, чтобы обеспечивать пользователю необходимый уровень их надежности, который может соотноситься с конкретной целью применения электронных подписей, например, получением государственных (муниципальных) услуг в цифровом формате, заключением сделок удаленно, дистанционным банковским обслуживанием, выполнением трудовых функции удаленно, взаимодействием с налоговыми или таможенными органами. С понятием надежности связано понятие доверия [8, с.117-119]. Каждому уровню обеспечения доверия соответствует та или иная степень надежности, связанная с определенными требованиями.

Принципиальный вопрос, касающийся доверенных сервисов, состоит в применении к ним уровней обеспечения надежности и доверия [10, с.40-44]. В ряде национальных законов об электронных подписях, а также региональном регулировании, например, в Постановлени eIDAS Европейского Союза [11], предусмотрены два уровня признания таких подписей. Первый уровень распространяется на все электронные подписи. Второй уровень предполагает признание определенных правовых последствий, таких как презумпция происхождения и целостности, за электронными подписями, удовлетворяющими определенным требованиям. Данное положение интерпретируется

как закрепление различных уровней обеспечения доверия применительно к электронным подписям. Постановления eIDAS может служить примером использования уровней обеспечения доверия в связи с выполнением требования идентификации при выдаче квалифицированного сертификата. А именно, требование о том, чтобы квалифицированный поставщик удостоверительных услуг проверил достоверность идентификационных данных лица, которому он выдает квалифицированный сертификат, может быть выполнено дистанционно с использованием средства электронной идентификации, имеющего «значительный» или «высокий» уровень обеспечения доверия.

Международные модели регулирования опираются на основополагающие принципы, разработанные Комиссией ООН по праву международной торговли (ЮНСИТРАЛ). Так, *принцип автономии сторон* означает для сторон свободу выбора при принятии ими решения относительно необходимого уровня обеспечения надежности/безопасности. Согласно п*ринципу технологической нейтральности* правовое регулирование не должно препятствовать инновациям вследствие конструирования юридических норм и правил, стимулирующих создание и внедрение одних технологий в ущерб другим. В соответствии с *принципом не дискриминации* юридическая сила и допустимость в качестве судебных доказательств электронных документов или электронных подписей не должны отвергаться только на основании электронной формы или не соответствия требованиям определенного уровня надежности/доверия. *Принцип функциональной эквивалентности* утверждает равнозначность юридических функций подписи независимо от электронного или бумажного носителя.

Результаты. В национальном законодательстве наряду с названными принципами реализуется, как правило, один из следующих методов регулирования. Императивный метод, далекий от технологической нейтральности и автономии сторон, гарантирует правовое признание только обеспечивающим высокий уровень надежности/доверия цифровым подписям. Примером реализации императивного метода в Российском законодательстве является Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 N 1-ФЗ (признан утратившим силу с 1 июля 2013 г. на основании ФЗ от 6 апреля 2011 г. N 63-ФЗ). Диспозитивный метод придерживается всех вышеуказанных принципов и придает юридическую значимость любым технологиям электронной подписи независимо от уровня их надежности. «Гибридный» метод соответствует гибкой модели регулирования [12, с.186-188]. Являясь в целом «технологически нейтральным» и «недискриминационным», он в первую очередь признает цифровые подписи, характеризующиеся высоким уровнем надежности /доверия.

Российское законодательство придерживается «гибридного» метода и гибкой модели регулирования, предусматривающей различные уровни требований к электронным подписям. Участники цифрового взаимодействия вправе использовать электронные подписи любого вида (ст.4 Федерального закона от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»). В соответствии ст.160 ГК РФ письменная форма сделки считается соблюденной при использовании электронной подписи любого вида. При этом усиленная квалифицированная подпись, характеризующаяся высоким уровнем доверия, имеет в силу закона юридическое значение в любых правоотношениях и предполагает признание определенных правовых последствий, таких как презумпция происхождения и целостности.

Во многих видах публичных и частных правоотношений законодатель предусмотрел использование квалифицированной электронной подписи, в том числе ее применение институтами защиты прав – судебной системой и нотариатом [13, с. 29-35]. Исковое заявление, заявление, жалоба, представление и иные документы, которые подаются посредством систем электронного документооборота участников процесса, должны быть подписаны усиленной квалифицированной электронной подписью. Для совершения нотариальных действий с электронными документами, а также передачи сведений, нотариальных документов в электронной форме, электронных образов нотариальных документов, созданных на бумажном носителе, в единую информационную систему нотариата нотариус использует усиленную квалифицированную электронную подпись. Банковская гарантия, представляемая в налоговый орган гарантом, подписывается усиленной квалифицированной электронной подписью лица, обладающего таким правом.

Безусловная юридическая значимость квалифицированной электронной подписи и доверие к ней базируются на строгих требованиях законодательства к электронной подписи данного вида, квалифицированному сертификату ключа проверки такой подписи, аккредитованному удостоверяющему центру (АУЦ).

Необходимо отметить, что юридические условия обеспечения доверенного цифрового взаимодействия постоянно обновляются и усложняются. К относительно новым условиям можно отнести порядок применения машиночитаемой доверенности. В законодательстве об электронной подписи закреплена правовая конструкция доверенности, выданной представителю в электронной форме в машиночитаемом виде, в том числе доверенности, выданной в порядке передоверия, а также удостоверенной квалифицированной подписью нотариуса (ст.187 ГК РФ; п.1.2) ст. 17.2. ФЗ «Об электронной подписи»). Машиночитаемая доверенность является частью системы обеспечения функциональной эквивалентности электронного документа его бумажному аналогу. В систему обеспечения юридической значимости электронного документа входят электронные реквизиты, которые указываются отправляющей стороной и проверяются стороной, получающей электронный документ, с помощью так называемых доверенных сервисов. Проверка наличия у лица, подписавшего электронный документ, полномочий на

подписание данных документов с помощью квалифицированной подписи также осуществляется в электронном виде. Правила предусматривают применение ключа подписи с полномочиями юридического лица только единоличным исполнительным органом, действующим без доверенности. При этом остальные сотрудники организации должны использовать для подписи и соответствующий ему закрытый ключ физических лиц. Для применения таких ключей подписей в служебных целях полномочия на их использование необходимо подтверждать с помощью электронного документа, называемого машиночитаемой доверенностью (МЧД). По аналогии с бумажной доверенностью на передачу права подписи МЧД подписывает генеральный директор (или другое лицо, которое может представлять организацию без доверенности) подписью юридического лица. МЧД формируется в виде структурированного XML-файла, который может быть прочитан программой. В случае использования доверенности в ограниченный промежуток времени или однократно МЧД прилагается к подписанному документу (пакету документов), а принимающая сторона анализирует документ и МЧД для принятия решения о корректности подписания и полномочиях подписавшего лица. В случае многократного использования МЧД, а также с целью обеспечения возможности ее оперативной отмены доверенность направляется на хранение в наиболее удобную для указанного использования информационную систему. Вместе с тем, попрежнему не решено значительное число организационных, технических и нормативных вопросов, в том числе вопросы наполнения и актуализации классификатора полномочий, которые необходимо решить для полноценного, надежного, отказоустойчивого использования машиночитаемых доверенностей во всех сегментах электронного взаимодействия. Препятствует созданию работоспособных юридических конструкций доверия технологическая, организационная и нормативная неопределенность в вопросах длительного архивного хранения документов с электронной подписью.

Ряд вопросов, связанных с обеспечением доверия, затрагивают тему ответственности сторон (удостоверяющих центров, владельцев сертификатов ключей проверки электронных подписей, доверенных третьих сторон и других), а именно: какие субъекты могут быть привлечены к ответственности; нормативные правовые механизмы ограничения ответственности, например, освобождение от бремени доказывания или перенос такого бремени; договорные ограничения ответственности.

В Российской Федерации согласно Федеральному закону от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» «удостоверяющий центр отвечает за последствия не предоставления услуг или неисполнения его функций в соответствии с требованиями закона или договора с владельцем сертификата ключа проверки электронной подписи. Аккредитованный удостоверяющий центр отвечает за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи, выданном таким удостоверяющим центром, или информации, содержащейся в реестре сертификатов, который ведет такой удостоверяющий центр». Представляется целесообразным ввести в российское право нормативные и договорные возможности ограничения ответственности субъектов, предоставляющих сервисы доверия.

В этой связи представляет интерес норма Положения eIDAS, которое вводит опровержимую презумпцию умысла или небрежности в отношении квалифицированного поставщика доверенных услуг, тогда как в отношении неквалифицированного поставщика бремя доказывания возлагается на лицо, требующее возмещения ущерба. Данная норма ставит целью укрепить доверие пользователей к квалифицированным сервисам, поскольку в случае возникновения ущерба эта презумпция упрощает взыскание возмещения. Наконец, признается право поставщика доверенных услуг ограничить свою ответственности при условии, что их клиенты заранее проинформированы об этих ограничениях и что эти ограничения признаются третьими сторонами.

К юридическим критериям, или факторам, доверия квалифицированной электронной подписи принадлежит федеральный государственный контроль (надзор), который направлен на предупреждение, выявление и пресечение нарушений обязательных требований. Применительно к сфере электронной подписи в полной мере справедливо утверждение С.М. Зырянова о том, что государственный контроль уделяет «значительное внимание профилактике нарушений обязательных требований. Однако сама по себе контрольно-надзорная деятельность, если она осуществляется систематически, формирует правовую среду, в которой контролируемым лицам более выгодно соблюдать обязательные требования» [14]. Федеральный государственный контроль (надзор) осуществляется Министерством цифрового развития, связи и массовых коммуникаций РФ в отношении аккредитованных удостоверяющих центров (АУЦ), а также в отношении аккредитованных доверенных третьих сторон в соответствии с Постановлением Правительства РФ от 29.06.2021 N 1044 (ред. от 29.08.2025) "Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере электронной подписи." Приказом Минцифры России от 7 декабря 2021 г. № 1312. утвержден перечень индикаторов риска нарушения обязательных требований при осуществлении государственного контроля. Минцифры России утверждены доклады о правоприменительной практике организации и осуществления федерального государственного контроля (надзора) в сфере электронной подписи в 2023 и 2024 годах. В режиме профилактических мероприятий Минцифры России постоянно проводит информирование граждан и организаций по наиболее часто возникающим вопросам законодательства РФ в

сфере электронной подписи. С целью укрепления доверия общества к цифровому взаимодействию с применением электронных подписей следует разработать специальный образовательный курс по практическому применению и юридическим аспектам электронной подписи, включая использование машиночитаемой доверенности (МЧД). Преподавание подобного курса целесообразно осуществлять в системе среднего специального и высшего образования.

Заключение. Информационно-коммуникационных технологий, которые лежат в основе цифровой экономики, позволяют гражданам и юридическим лицам быстро и эффективно взаимодействовать в цифровой среде с государственными органами и организациями частного сектора, участвовать в предпринимательской и некоммерческой деятельности, защищать свои права и законные интересы. Дистанционный формат предполагает применение специальных юридических конструкций, при помощи которых достигается определенность в отношении подтверждения личности, правомерности, юридической силы и последствий онлайн операций, то есть устанавливается доверие участников и общества в целом к результатам экономической и социальной деятельности в цифровой среде. Ключевым юридическим механизмом, обеспечивающим доверие, является применение электронных подписей. Правовое регулирование электронных подписей базируется на технологических и юридических принципах и требованиях, а также механизмах ответственности, чтобы обеспечивать пользователю достаточный уровень уверенности в их надежности. Юридические условия доверенного цифрового взаимодействия постоянно обновляются и усложняются.

Безусловная юридическая значимость квалифицированной электронной подписи и доверие к ней базируются на строгих требованиях законодательства к электронной подписи данного вида, аккредитованному удостоверяющему центру, порядку применения машиночитаемой доверенности, механизмах ответственности. К юридическим критериям, или факторам, доверия квалифицированной электронной подписи принадлежит федеральный государственный контроль (надзор), который направлен на побуждение соблюдения обязательных требований. Вместе с тем правовое регулирование электронных подписей не свободно от недостатков и требует совершенствования. Необходимо устранить технологическую, организационную и правовую неопределенность в вопросах длительного архивного хранения документов с электронной подписью. Представляется целесообразным ввести в российское право нормативные и договорные возможности ограничения ответственности субъектов, предоставляющих сервисы доверия. С целью укрепления доверия общества к цифровому взаимодействию с применением электронных подписей следует разработать специальный образовательный курс по практическому применению и юридическим аспектам электронной подписи Преподавание подобного курса целесообразно осуществлять в системе среднего специального и высшего образования.

Необходимо также принимать во внимание проблему общего характера. В российском законодательстве используются конструкции, относящиеся к сфере правового регулирования доверенного цифрового взаимодействия**.** Однако в федеральном законодательстве отсутствует общее понятие «доверенное взаимодействие», его дефиниция и концептуальная проработка. Следует установить на уровне федерального законодательства, что означает «доверие» применительно к указанной сфере и определить данное понятие, учитывая широкое социально-психологическое и юридическое понимание доверия.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Васильева Т.А. Внедрение информационных технологий в парламентскую деятельность// Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 9 (97). С. 93-101. DOI: 10.17803/2311-5998.2022.97.9.093-101 EDN: PHNEQA

2. Биткова Л.А., Устюкова В.В. Правовое регулирование применения информационных систем в сельском хозяйстве//Экономика сельского хозяйства России. 2022. № 9. С. 37-41. DOI: 10.32651/229-37 EDN: MCZQPZ

3. Андреев В.К. Вопросы теории правового регулирования предпринимательства в условиях цифровизации//Журнал российского права. 2022. Т. 26. № 2. С. 36-47. DOI: 10.12737/jrl.2022.015 EDN: FTGPDB

4. Клеандров М. И. Цифровая экономика и проблемы механизма правосудия// Экономика. право. Общество. 2018. № 1 (13). С.28-35. EDN: XYLKBN

5. Куделькин Н.С. Традиционное природопользование и охрана окружающей среды севера (часть 1) //Юридические исследования. 2025. № 11. С. 23-38. DOI: 10.25136/2409-7136.2025.11.76653 EDN: DTBWTH

6. Дубень А.К. Эектронное правосудие в цивилистическом процессе на примере института судебного извещения//Образование и право. 2025. № 5. С. 391-395. DOI: 10.24412/2076-1503-2025-5-391-395 EDN: KHCVWT

7. Летова Н.В., Соловяненко Н.И. Государственная социальная помощь отдельным категориям граждан: цифровой разрыв и юридические способы его преодоления // Закон. 2024. № 12. С. 66-72. DOI: 10.37239/0869-4400-2024-21-12-66-72 EDN: OVSBZO

8. Соловяненко Н.И. Взаимосвязь категорий "надежность" и "ответственность" в системе правового регулирования и применения электронной подписи.

9. Проблемы экономики и юридической практики. 2025. Т. 21. № 5. С. 116-121. DOI: 10.33693/2541-8025-2025-21-5-116-121 EDN: YJKXEH

10. Корсик К.А. Цифровые права как новые объекты гражданских прав и новые правила о соблюдении письменной формы сделки // Нотариальный вестник. 2019. № 4. EDN: ZDBJXF

11. Сабанов А.Г., Аутентификация как составляющая единого пространства доверия // Электросвязь. 2012. № 8. С. 40-44. EDN: PBCMWH

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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

13. Чуча С.Ю. Некоторые особенности обеспечения занятости в условиях гибридного правоприменения // Право и государство: теория и практика. 2025. № 3. С. 186-188. DOI: 10.47643/1815-1337_2025_3_186 EDN: YOOGUS

14. Чуча С.Ю. Правовой режим электронных доказательств в суде при рассмотрении трудовых споров // Предпринимательское право. 2019. № 3. С. 29-35. EDN: TNJYZL

15. Зырянов, С. М. Место и роль государственного контроля (надзора) в механизме правового регулирования / С. М. Зырянов // Административное право и процесс. - 2025. - № 4. - С. 15-21. DOI: 10.18572/2071-1166-2025-4-15-21 EDN: TLZRDM

References

1. Vasilyeva T.A. Introduction of information technologies in parliamentary activity// Bulletin of the O.E. Kutafin University (MGUA). 2022. № 9 (97). Pp. 93-101. DOI: 10.17803/2311-5998.2022.97.9.093-101 EDN: PHHEQA

2. Bitkova L.A., Ustyukova V.V. Legal regulation of the use of information systems in agriculture//The economics of agriculture in Russia. 2022. No. 9. pp. 37-41. DOI: 10.32651/229-37 EDN: MCZQPZ

3. Andreev V.K. Issues of the theory of legal regulation of entrepreneurship in the context of digitalization//Journal of Russian Law. 2022. Vol. 26. No. 2. pp. 36-47. DOI: 10.12737/jrl.2022.015 EDN: FTGPDB

4. Kleandrov M. I. Digital economy and problems of the justice mechanism// Economy. right. Society. 2018. No. 1 (13). pp.28-35. EDN: XYLKBN

5. Kudelkin N.S. Traditional nature management and environmental protection of the North (part 1) //Legal research. 2025. No. 11. pp. 23-38. DOI: 10.25136/2409-7136.2025.11.76653 EDN: DTBWTH

6. Duben A.K. Electronic justice in the civil process on the example of the institution of judicial notification//Education and law. 2025. No. 5. PP. 391-395. DOI: 10.24412/2076-1503-2025-5-391-395 EDN: KHCVWT

7. Letova N.V., Solovyanenko N.I. State social assistance to certain categories of citizens: the digital divide and legal ways to overcome it // Law. 2024. No. 12. pp. 66-72. DOI: 10.37239/0869-4400-2024-21-12-66-72 EDN: OVSBZO

8. Solovyanenko N.I. Interrelation of the categories "reliability" and "responsibility" in the system of legal regulation and application of electronic signatures.

9. Problems of economics and legal practice. 2025. Vol. 21. No. 5. Pp. 116-121. DOI: 10.33693/2541-8025-2025-21-5-116-121 EDN: YJKXEH

10. Korsik K.A. Digital rights as new objects of civil rights and new rules on compliance with the written form of the transaction // Notary Bulletin. 2019. No. 4. EDN: ZDBJXF

11. Sabanov A.G., Authentication as a component of a single trust space // Telecommunication. 2012. No. 8. pp. 40-44. EDN: PBCMWH

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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

13. Chucha S.Y. Some features of employment provision in the context of hybrid law enforcement // Law and the State: theory and practice. 2025. No. 3. PP. 186-188. DOI: 10.47643/1815-1337_2025_3_186 EDN: YOOGUS

14. Chucha S.Y. The legal regime of electronic evidence in court when considering labor disputes // Business law. 2019. No. 3. pp. 29-35. EDN: TNJYZL

15. Zyryanov, S. M. The place and role of state control (supervision) in the mechanism of legal regulation / S. M. Zyryanov // Administrative law and Process. - 2025. - No. 4. - pp. 15-21. DOI: 10.18572/2071-1166-2025-4-15-21 EDN: TLZRDM

Информация об авторах:

Соловяненко Нина Ивановна, кандидат юридических наук, старший научный сотрудник сектора процессуального права Института государства и права Российской академии наук; Nina.coshkina@yandex.ru

Nina I. Solovyanenko, PhD in Law, Senior Researcher at the Procedural Law Branch of the Institute of State and Law of the Russian Academy of Sciences

Статья поступила в редакцию / The article was submitted 12.11.2025;
Одобрена после рецензирования / Approved after reviewing 13.12.2025;
Принята к публикации / Accepted for publication 20.12.2025.
Автором окончательный вариант рукописи одобрен.