УДК 341.17 DOI: 10.22394/2074-7306-2020-1-1-110-116

ЮРИДИЧЕСКАЯ РОЛЬ ЦИФРОВОГО «ПРОСТРАНСТВА ДОВЕРИЯ» В ФОРМИРОВАНИИ «ПРОСТРАНСТВ ЗНАНИЙ» ИНТЕГРАЦИОННЫХ ОБЪЕДИНЕНИЙ ГОСУДАРСТВ (ЕС и ЕАЭС)[1]

Соловяненко Нина Ивановна кандидат юридических наук, старший научный сотрудник сектора предпринимательского и корпоративного права, Институт государства и права Российской академии наук (119019, Россия, г. Москва, Знаменка,10).
E-mail: nina.coshkina@yandex.ru.

Аннотация

В работе рассматриваются правовые вопросы обеспечения доверия для цифрового взаимодействия в «пространствах знаний», охватывающих сферу образования, научных исследований и инноваций в интеграционных объединениях государств (ЕС и ЕАЭС). Выделены обязательные юридические условия для развития «пространства знаний» в цифровой среде – безопасность и правовая определенность цифрового взаимодействия. Анализируются основные юридические конструкции доверия: управление идентификационными данными и удостоверительные услуги. Обозначена необходимость создания правовой основы трансграничного пространства доверия в виде международного соглашения, а также соответствующего национального законодательства.

Ключевые слова: *устойчивое развитие, образование, научные исследования, инновации, пространства знаний, пространства доверия, интеграционные объединения государств, доверенные услуги, управление идентификационными данными, нормативные и технические условия доверия, правовая основа трансграничного пространства доверия.*

В течение последних десятилетий наблюдается процесс усовершенствования всеобщего доступа к знаниям в цифровом пространстве, охватывающий в том числе сферу образования, научных исследований и инноваций. Названное явление особо отмечается в посвященных выполнению глобальной программы устойчивого развития документах международных межправительственных организаций. В рекомендациях ЮНЕСКО под цифровым пространством (или киберпространством) понимается виртуальный мир цифровой или электронной коммуникации, связанной с глобальной информационной инфраструктурой, а всеобщим признается доступ для всех граждан к информационной инфраструктуре (в частности, к Интернету) и к информации и знаниям, необходимым для развития общества и личности[2]. Использование информационно-коммуникационных технологий для создания новых знаний во всех областях науки, публикации результатов научных исследований, исследовательских данных в цифровом формате, а также в целях модернизации методов управления наукой и научными исследованиями привлекает повышенное внимание со стороны академического сообщества, правительств, организаций гражданского общества, а также частного бизнеса.

Сообразно целям устойчивого развития перед государствами-членами ООН и международными организациями поставлены задачи внедрения информационно-коммуникационных технологий и глобального подключения сетей и в итоге – преодоления «цифрового разрыва» и формирования общества, основанного на знаниях[3]. Так, ЮНЕСКО уделяет особое внимание удовлетворению потребностей в инфокоммуникациях общественных служб и учебных заведений. В этой связи государствам рекомендуется совершенствовать системы хранения и перевода в цифровой формат информации и знаний, являющихся общественным достоянием, создавая тем самым образовательную и научную среду, способствующую творческому подходу и расширению аудитории. Причем расходы, связанные с использованием телекоммуникаций, должны быть посильными с учетом льготных тарифов для публичных организаций: школ, академических учре-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-15014 «Эффективность правового регулирования процессов формирования «зоны знаний» интеграционных объединений государств (на примере сравнительно-правового исследования ЕС и ЕАЭС)».

[2] The Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace was adopted by the UNESCO General Conference at its 32nd session in Paris on 15 October 2003. URL:https://en.unesco.org/themes/linguistic-diversity-and-multilingualism-internet/recommendation.

[3] «Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года». URL:https://www.un.org/sustainabledevelopment/ru/about/development-agenda.

ждений, музеев, архивов и библиотек. Рекомендуется также активизировать работу и содействовать распространению знаний и навыков в области использования цифровых технологий, в том числе путем укрепления доверия в вопросах разработки и применения этих технологий[1].

В интеграционных объединениях государств, таких как ЕС и ЕАЭС, утверждены основополагающие юридические документы, регламентирующие развертывание «цифровых пространств», соотносимых с «пространствами знаний» – цифровые повестки дня [1; 2]. В них воплощены в целом универсальные, гармонизированные правовые подходы к инновационному цифровому развитию, которых придерживаются государства в рамках интеграционных объединений.

Универсальным правовым подходом является законодательная поддержка научных исследований и инноваций, создание наилучших юридических условий для наращивания «пространства знаний» за счет применения информационно-коммуникационных технологий, которые рассматриваются законодателем в качестве основы современных инновационных систем[2].

В Евразийском Союзе в 2009 году принята «Концепция создания Евразийской инновационной системы», которая представляет собой совокупность институтов, обеспечивающих формирование инфраструктурных элементов, норм и правил регулирования межгосударственных отношений в сфере инновационной деятельности. В основе Евразийской инновационной системы заложены базовые принципы государственной политики членов ЕАЭС: поддержка и стимулирование инновационной деятельности; развитие национальных инновационных систем; координация и сотрудничество при разработке и реализации межгосударственных целевых программ и инновационных проектов. В стратегическом документе «Основные направления реализации цифровой повестки ЕАЭС до 2025 года» определены принципы, задачи и механизмы сотрудничества государств-членов по вопросам цифровой повестки и формирования единого цифрового пространства Союза, которое интегрирует информационные ресурсы, а также совокупность цифровых инфраструктур, цифровые процессы и средства цифрового взаимодействия.

В Европейском Союзе наилучшие условия для научных исследований и инноваций формируются, начиная с процесса проектирования политических решений, стратегий и нормативных правовых актов. При разработке Европейской комиссией новых законодательных инициатив обязательно учитывается их влияние на инновационную деятельность. Воздействие новых технологий на регулирование в ЕС также подлежит тщательному изучению на ранних стадиях законодательного процесса. Примерами могут служить искусственный интеллект или блокчейн, под влиянием которых планируются изменения в законодательстве. Нормотворческие инициативы ЕС соотносятся с потребностями инновационных компаний, которым предоставляются необходимые данные для оценки регулятивного воздействия, а также учитываются их рекомендации при разработке законодательства. Европейская комиссия в целях корректировки действующих правил ЕС проводит инновационные консультации, в ходе которых определяется, является ли политика, стратегия или регулирование ЕС препятствием для инноваций, и если да, то ведется поиск соответствующего решения. Такая практика позволяет Европе располагать благоприятным, «дружелюбным» в отношении научных изысканий и инноваций законодательством («Research and Innovation friendly regulation»)[3].

Данный правовой подход применяется в том числе при разработке дорожной карты реализации Европейского открытого научного облака (EOSC), принятой Европейской комиссией в 2018 году, и стратегического плана внедрения ЭОSC, опубликованного в 2019 году. Назначение ЭОSC заключается в создании «глобальной структуры данных», которые в результате стандартизации, хранения и обработки могут использоваться учеными и другими заинтересованными лицами. Правовая модель EOSC предусматривает свободный доступ к результатам исследований, проведенных за счет государственного финансирования. Европейская облачная инициатива основывается на стратегии цифрового единого рынка[4] и предполагает формирование доверенной, открытой среды для научного сообщества в целях получения, обмена и повторного использования науч-

[1] The Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace was adopted by the UNESCO General Conference at its 32nd session in Paris on 15 October 2003. URL:https://en.unesco.org/themes/linguistic-diversity-and-multilingualism-internet/recommendation

[2] A Digital Single Market Strategy for Europe. /* COM/2015/0192 final URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[3] Research and Innovation friendly regulation - Council conclusions (adopted on 27/05/2016). URL:http://data.consilium.europa.eu/doc/document/ST-9510-2016-INIT/en/pdf.

[4] A Digital Single Market Strategy for Europe. Brussels, 6.5.2015. URL:https://ec.europa.eu/digital-single-market/en/news/digital-single-market-strategy-europe-com2015-192-final.

ных результатов, создания коллективных научных знаний и управления научными исследованиями в странах ЕС. Дорожная карта включает шесть направлений разработки EOSC: а) архитектура, б) данные, в) услуги, г) доступ и интерфейсы, д) правила и е) управление[1]. Развертывание EOSC принадлежит к числу политико-правовых приоритетов для формирования общеевропейского «пространства знаний».

Создание наилучших юридических условий для функционирования цифрового «пространства знаний» означает, что правовое регулирование должно отвечать общественным интересам наравне с уровнем развития технологий, исполнять юридическую функцию прежде всего по усилению безопасности и правовой определенности цифрового взаимодействия. В этой связи на глобальном уровне, а также в рамках объединений экономической интеграции и в отдельных государствах поставлена фундаментальная юридическая задача – правовое обеспечение доверия в цифровой среде. Страны – члены Организации экономического сотрудничества и развития (ОЭСР) констатировали, что гарантии доверия наряду с управлением рисками безопасности и конфиденциальности являются ключевыми элементами, необходимыми для экономического и социального развития в условиях цифровой трансформации[2].

Правовая основа инновационной стратегии как в ЕС, так и в ЕАЭС включает нормативное регулирование, поддерживающее формирование доверенной среды для сферы образования, науки и инновационной деятельности. В материалах Комиссии ООН по праву международной торговли (ЮНСИТРАЛ) также подчеркивается, что, поощряя доверие к онлайн-пространству, такая правовая основа является фактором, способствующим достижению целей устойчивого развития в сфере содействия инновациям[3].

Для укрепления названного фактора требуется единообразная система правил, начиная с понятийного аппарата. В этой связи в интеграционных объединениях государств разработаны и закреплены в юридических документах такие понятия, как: «доверенная третья сторона», «доверенные услуги (сервисы доверия)», а также обобщающее понятие «пространство доверия». Необходимо указать, что «пространство доверия» проектируется равно как внутригосударственное, так и трансграничное. В Евразийском Союзе на основе Договора о ЕАЭС (Протокол об информационно-коммуникационных технологиях и информационном взаимодействии в рамках ЕАЭС) предусмотрено формирование «трансграничного пространства доверия» в целях информационного обеспечения интеграционных процессов во всех сферах, затрагивающих функционирование Союза. Трансграничное «пространство доверия» определено как «совокупность правовых, организационных и технических условий, согласованных государствами-членами с целью обеспечения доверия при межгосударственном обмене данными и электронными документами».

Признанию иностранных и международных конструкций доверия способствует наличие внутригосударственной основы – правовых условий такого признания. Например, российский закон «Об электронной подписи» содержит правила признания электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами. В правоотношениях, регулируемых российским законодательством, такое признание осуществляется в соответствии с международными договорами РФ. Подтверждение соответствия электронных подписей требованиям международных договоров может производиться в том числе аккредитованной доверенной третьей стороной, уполномоченной международным договором РФ.

Трансграничное признание упрощается, когда внутреннее законодательство государств содержит правовые нормы, основанные на общих принципах, или идентичные положения. По этим причинам ЮНСИТРАЛ разрабатывает правовую основу трансграничного пространства доверия в виде международного соглашения, а также типового законодательства для принятия на внутригосударственном уровне[4].

Базовым юридическим компонентом доверия является правовая конструкция идентификации и аутентификации участников цифрового взаимодействия в режиме онлайн. В документах ЮНСИТРАЛ под «электронной идентификацией» понимается процедура использования иденти-

---

[1] European Open Science Cloud: Strategic Implementation Plan. Luxembourg: Publication Office of the European Union, 2016. Doi:10.2777/940154

[2] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris. 21–38 DOI: https://dx.doi.org/10.1787/9789264276284-en.

[3] Draft Instrument on Cross-Border Legal Recognition of Identity Management and Trust Services - Proposal by Germany URL:https://undocs.org/en/A/CN.9/WG.IV/WP.155.

[4] Draft Provisions on the Cross-border Recognition of IdM and Trust Services. URL:https://undocs.org/en/A/CN.9/WG.IV/WP.157.

фикационных данных в электронной форме, уникально представляющих физическое или юридическое лицо, либо физическое лицо, представляющее юридическое лицо. В свою очередь «аутентификация» означает процесс, который позволяет производить электронную идентификацию физического или юридического лица, или же подтверждение происхождения и целостности данных в электронной форме[1].

Юридическая роль идентификации и аутентификации признается как в национальном, так и в международном праве. В стратегии ООН в области устойчивого развития на период до 2030 года предусмотрено обеспечение наличия у всех людей законных удостоверений личности. В цифровой экономике юридическая функция идентификации (удостоверения) личности реализуется посредством использования идентификационных данных в цифровой форме.

Идентификация необходима для решения различных юридических задач в электронной среде: соблюдения требований законодательства, установления действительности документа, выполнения договорных обязательств, защиты интеллектуальной собственности. Российский федеральный закон от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» регулирует применение информационных технологий в целях идентификации граждан РФ. Закон закрепил понятие единой системы идентификации и аутентификации (ЕСИА) – федеральной государственной информационной системы, которая обеспечивает санкционированный доступ к информации, содержащейся в информационных системах. Порядок регистрации гражданина РФ в единой системе идентификации и аутентификации, включая состав необходимых для регистрации сведений, порядок и сроки проверки и обновления сведений, размещаемых в ЕСИА с использованием государственных информационных систем, устанавливаются Правительством РФ. В российском законодательстве об электронной подписи зафиксирована обязанность аккредитованного удостоверяющего центра установить личность физического лица, обратившегося к нему за получением квалифицированного сертификата электронной подписи, а также направить в ЕСИА сведения о лице, получившем квалифицированный сертификат.

Аналогичные по содержанию положения содержатся в зарубежном, в том числе европейском, законодательстве, прежде всего в «Регулировании № 910/2014 Европейского парламента и Совета «Об электронной идентификации и доверенных услугах для электронных транзакций на внутреннем рынке и отмене Директивы 1999/93/ЕС» (eIDAS regulation). По смыслу регулирования идентификация субъектов в онлайновом режиме представляет собой услугу управления идентификационными данными. Субъект, ответственный за идентификацию физических или юридических лиц, выдачу соответствующих средств идентификации, а также управление идентификационной информацией (идентификационными данными), выполняет функцию «поставщика идентификационных услуг». Последний может быть частным или публичным. В правоотношениях по установлению личности с помощью средств идентификации применяется такая категория, как «уровни обеспечения безопасности средств электронной идентификации». Уровни безопасности подразделяются на «низкий», «существенный» и «высокий» и нацелены, соответственно, на снижение риска ненадлежащего использования или изменения идентификационных данных; существенное снижение такого риска; предотвращение ненадлежащего использования или изменения идентификационных данных. Таким образом, определение правовых последствий, вытекающих из электронной идентификации, в соответствии с каждым уровнем безопасности позволит заинтересованным сторонам уменьшить свои юридические риски, выбрав наиболее подходящий уровень безопасности и правовые последствия в соответствии со своими потребностями. Чем выше уровень обеспечения безопасности, тем более благоприятные правовые последствия будут возникать для пользователя услуг, включая режим ответственности поставщика соответствующих услуг.

Соблюдение необходимых требований безопасности обеспечивается посредством применения различных технологий. Вместе с тем подобные требования устанавливаются с учетом принципа технологической нейтральности законодательства.

Надежная идентификация требуется при осуществлении цифрового взаимодействия как в коммерческих, так и некоммерческих секторах. В условиях Европейского открытого научного облака исследователи могут получать доступ к сетевым ресурсам с помощью единого набора идентификационных данных для входа, предоставляемых и управляемых их собственными учреждениями. Например, для библиотек это означает, что исследователь, принадлежащий к учреждению, может использовать механизм единого входа (SSO) для доступа к электронным ресурсам, на которые подписана библиотека. Пользователям, как только они нашли нужный электронный ресурс

[1] Draft Provisions on the Cross-border Recognition of IdM and Trust Services. URL:https://undocs.org/en/A/CN.9/WG.IV/WP.157.

(журнал или статью в журнале) и получили доступ к нему со своими идентификационными данными, не нужны другие идентификационные данные при переходе на иные ресурсы. Они могут получить доступ из любого места и с помощью любого устройства. SSO доступна во многих университетах и научно-исследовательских институтах Европы. Однако требуют решения ряд проблем, таких, как определение учетных данных, необходимых для получения разных видов услуг, установление уровней доверия к учетным данным, требуемым различными службами [3].

Правила электронной идентификации ЕС (eIDAS regulation) действуют в отношении Европейской инициативы по студенческим картам. Каждый студент – владелец карты имеет право идентифицировать и зарегистрировать себя в электронном виде в высших учебных заведениях Европы при переезде за границу для получения образования. Электронная идентификация устраняет обязательную процедуру регистрации на месте и бумажный документооборот. Кроме того, карта позволит студентам получить право доступа к онлайн-курсам и услугам, предоставляемым в других высших учебных заведениях. Данная инициатива рассматривается специалистами как существенный элемент цифрового европейского образовательного пространства[1].

В международных документах отмечается непосредственная технологическая и юридическая взаимосвязь между услугами по управлению идентификационными данными и так называемыми электронными «удостоверительным услугами».

В европейском законодательстве установлен открытый перечень удостоверительных услуг, к которым относятся: а) создание, проверка и подтверждение электронных подписей, электронных печатей или электронных отметок времени; электронная доставка и выдача сертификатов, связанных с этими услугами; б) создание, проверка и подтверждение сертификатов, удостоверяющих подлинность веб-сайтов; в) хранение электронных подписей, печатей или сертификатов, связанных с этими услугами. Так, например, услуги подтверждения подлинности веб-сайтов позволяют посетителю веб-сайта убедиться, что данный веб-сайт принадлежит надлежащему лицу. Услуги, связанные с электронными печатями, позволяют подтвердить, что документ исходит от определенного юридического лица, обеспечивая, таким образом, доказательства происхождения и достоверности документа. Услуги долговременного хранения электронных подписей, печатей должны гарантировать действительность электронных подписей и электронных печатей в течение длительного срока и возможность их подтверждения вне зависимости от технологических изменений в будущем. Услуги электронной доставки с подтверждением получения создают презумпцию целостности электронных документов, отправки таких документов идентифицированным отправителем, их получения идентифицированным получателем, подтверждения даты и времени отправки и получения.

В правовых документах Евразийского Союза, в том числе «Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов» предусматривается использование в рамках ЕАЭС удостоверительных услуг (доверенных сервисов).

Система правил для обеспечения безопасности и юридической определенности отношений в области управления идентификационными данными и удостоверительных услуг является основополагающей для всех электронных операций. Значение соответствующей нормативной базы, а также методических рекомендаций для снижения рисков и формирования доверия к подлинности взаимодействующих сторон отмечается как правоведами [4; 5; 6], так и специалистами в области информационных технологий [7].

Отношения в области управления идентификационными данными и удостоверительных услуг не свободны от правовых препятствий как на международном, так и национальном уровне. В их числе: отсутствие законодательных положений, придающих юридическую силу и правовую определенность таким отношениям; различия в законах и правовых подходах к управлению идентификационными данными; законодательные положения, основанные на специфических технологических требованиях; нормативные предписания в отношении представления бумажных документов для осуществления юридического взаимодействия; отсутствие механизмов трансграничного юридического признания идентификационных данных и удостоверительных услуг.

Соответственно, необходимо разработать совокупность правовых инструментов и конструкций, способствующих преодолению названных препятствий и созданию благоприятных правовых условий для оказания идентификационных и удостоверительных услуг в режиме онлайн. В российское право указанные инструменты и конструкции целесообразно интегрировать

[1] European student card initiative. URL:https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en

при обновлении информационного законодательства (например, при разработке информационного кодекса или закона об электронном документе). На международном уровне представляется целесообразным разработать институциональный механизм сотрудничества в обеспечении функциональной совместимости и безопасности управления идентификационными данными и удостоверительных услуг, в частности, в отношении технических требований и уровней обеспечения доверия. Разработка международно-правовых подходов и решений будет стимулировать трансграничное взаимодействие между системами управления идентификационными данными и удостоверительными услугами независимо от их частной или государственной принадлежности.

Литература

1. *Соловяненко Н.И.* Цифровая повестка дня в правовом механизме формирования «пространства знаний» в интеграционных объединениях государств (ЕС и ЕАЭС) //Гуманитарные, социально-экономические и общественные науки. 2019 г. № 8. С. 163 – 167.
2. *Scott e al., M.*, Contribution to growth: The European Digital Single Market. Delivering economic benefits to citizens and businesses, Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2018. URL:https://bruegel.org/wp-content/uploads/2019/02/IPOL_STU2019631044_EN.pdf.
3. *Garibyan M.* Access and identity management for libraries: controlling access to online information / *M. Garibyan, S. McLeish, J. Paschoud.* London: Facet Publishing, 2014. 248 с.
4. *Наумов В.Б.* Проблемы развития законодательства об идентификации субъектов информационных отношений в условиях цифровой экономики // Труды Института государства и права РАН. № 4/2018. С. 125 – 151.
5. *Полякова Т.А., Минбалеев А.В., Бойченко И.С.* Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права//Вестник УрФО. Безопасность в информационной сфере. 2019. № 3 (33). С. 64 – 68.
6. *Шапсугова М.Д.* Реализация принципов цифровой экономики и технологии смарт-контрактов в правовом регулировании предпринимательской деятельности // Северо-Кавказский юридический вестник. 2018. № 2. С. 76 – 82.
7. *Минаев В.А., Королев И.Д., Сабанов А.Г.* Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия//Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 43 – 49.

Solovyanenko Nina Ivanovna, Candidate of Legal Sciences, Senior Research Fellow of the Business and Corporate Law Department, Institute of State and Law, Russian Academy of Sciences (10, Znamenka, Moscow, 119019, Russian Federation).
E-mail: nina.coshkina@yandex.ru

THE LEGAL ROLE OF THE DIGITAL «ENVIRONMENT OF TRUST» IN THE FORMATION OF OF «KNOWLEDGE SPACES» OF INTEGRATION ASSOCIATIONS OF STATES (EU and EEU)

Abstract

The paper deals with legal issues of ensuring trust for digital interaction in the "knowledge spaces" covering the sphere of education, research and innovation, in integration associations of States (the EU and the EEU). Mandatory legal conditions for the development of the "knowledge space" in the digital environment - security and legal certainty of digital interaction-are highlighted. The main legal structures of trust are analyzed: identity management and trust services. The necessity of creating a legal basis for a cross-border «environment of trust» in the form of an international agreement, as well as relevant national legislation, is indicated.

Key words: *sustainable development, education, research, innovation, knowledge spaces, environment of trust, integration associations of States, trust services, identity management, regulatory and technical conditions of trust, legal basis for a transboundary environment of trust.*

References

1. Solovyanenko N.I. Cifrovaya povestka dnya v pravovom mekhanizme formirovaniya «prostranstva znanij» v integracionnyh ob"edineniyah gosudarstv (ES i EAES) //Gumanitarnye, social'no-ekonomicheskie i obshchestvennye nauki. 2019 g. № 8. S. 163 – 167.
2. Scott e al., M., Contribution to growth: The European Digital Single Market. Delivering economic benefits to citizens and businesses, Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European

Parliament, Luxembourg, 2018. URL:https://bruegel.org/wp-content/uploads/2019/02/IPOL_STU2019631044_EN.pdf.
3. Garibyan M. Access and identity management for libraries: controlling access to online information / M. Garibyan, S. McLeish, J. Paschoud. London: Facet Publishing, 2014. – 248 c.
4. Naumov V.B. Problemy razvitiya zakonodatel'stva ob identifikacii sub"ektov informacionnyh otnoshenij v usloviyah cifrovoj ekonomiki // Trudy Instituta gosudarstva i prava RAN. № 4/2018. S. 125 – 151.
5. Polyakova T.A., Minbaleev A.V., Bojchenko I.S. Konceptual'nye podhody k pravovomu regulirovaniyu informacionnoj bezopasnosti v usloviyah cifrovizacii i transformacii prava// Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2019. № 3 (33). S. 64 – 68.
6. SHapsugova M.D. Realizaciya principov cifrovoj ekonomiki i tekhnologii smart-kontraktov v pravovom regulirovanii predprinimatel'skoj deyatel'nosti// Severo-Kavkazskij yuridicheskij vestnik. 2018. № 2. S. 76 – 82.
7. Minaev V.A., Korolev I.D., Sabanov A.G. Ocenka riskov identifikacii i autentifikacii sub"ektov elektronnogo vzaimodejstviya//Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2018. № 4 (30). S. 43 – 49.

УДК 347 DOI: 10.22394/2074-7306-2020-1-1-116-121

О СОВЕРШЕНСТВОВАНИИ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ, РЕГУЛИРУЮЩЕГО АКЦЕССОРНЫЕ ОБЯЗАТЕЛЬСТВА

Евсеева Людмила Анатольевна кандидат юридических наук, доцент, зав. кафедрой частного права, Чебоксарский кооперативный институт (филиал) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации»
(428025, Россия, г. Чебоксары, пр. М. Горького, д. 24).
E-mail: evseeva-ludmila@yandex.ru

Трухан Роман Петрович аспирант, Чебоксарский кооперативный институт (филиал) автономной некоммерческой образовательной организации высшего образования Центросоюза Российской Федерации «Российский университет кооперации»
(428025, Россия, г. Чебоксары, пр. М. Горького, д. 24).
E-mail: 79224673495@yandex.ru

Аннотация

В статье рассматриваются российская правовая модель акцессорных обязательств и перспективы ее развития. Отмечены недостатки действующей редакции Гражданского кодекса Российской Федерации, в которой отсутствует системное регулирование данного вида обязательств. Сделан вывод о целесообразности включения в кодекс статьи, закрепляющей деление обязательств на основные и дополнительные (акцессорные), а также существенные признаки данных видов обязательств. Сформулированы основные концептуальные положения данной статьи. Кроме того, критическому анализу подвергнута статья 329 Гражданского кодекса Российской Федерации, а также нормы отдельных законодательных актов, регулирующих способы обеспечения исполнения обязательств, изложены предложения по их совершенствованию.

Ключевые слова: *гражданское право, гражданско-правовая природа обязательств, основные обязательства, дополнительные обязательства, акцессорные обязательства, акцессорность действительности, обеспечение исполнения обязательств, способы обеспечения обязательств, обеспечительная сделка, независимая гарантия, гарантийное обязательство.*

Исходным ключевым недостатком российского законодательства, регулирующего акцессорные обязательства, является отсутствие в нем норм, конституирующих данный вид обязательств как таковых. Сложилась парадоксальная ситуация: суды активно ссылаются на акцессорную природу обязательств, прежде всего обеспечительных, в то время как свойство акцессорно-