

Научная статья
УДК 342
DOI 10.33184/pravgos-2022.3.22

Original article

ХИМЧЕНКО Алексей Игоревич
Московский государственный
юридический университет
им. О.Е. Кутафина (МГЮА),
Москва, Россия;
e-mail: alekseykhimchenko@yandex.ru;
<https://orcid.org/0000-0003-1171-6023>

KHIMCHENKO Aleksey Igorevich
Kutafin Moscow State Law University (MSAL),
Moscow, Russia.

ВОПРОСЫ ФОРМИРОВАНИЯ ЦИФРОВОЙ СРЕДЫ ДОВЕРИЯ КАК СТРУКТУРНОГО ЭЛЕМЕНТА В ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

ISSUES OF CREATING THE DIGITAL ENVIRONMENT OF TRUST AS A STRUCTURAL
ELEMENT IN THE DIGITALIZATION OF PUBLIC ADMINISTRATION

Аннотация. Статья посвящена исследованию правовых аспектов цифровой среды доверия, выявлению тенденций и проблем, связанных с особенностями ее формирования в условиях цифровизации государственного управления. В процессе цифровой трансформации государственного управления происходит видоизменение форм и механизмов реализации, формирование новых инструментов взаимодействия. Возникающая при этом тенденция повышения роли дистанционных коммуникаций требует научного осмысления имеющихся проблем в целях формирования цифровой среды доверия. Цели исследования: анализ механизмов реализации доверенных коммуникаций, формирование предложений по стимулированию цифровой среды доверия. Методы исследования: анализа, системный, абстрагирования, построения гипотез, идеализации, правового моделирования, сравнительно-правовой. Результаты: в статье выделяются векторы развития механизмов доверенных коммуникаций, анализируются текущая ситуация и проблемные вопросы, формулируются предложения по формированию цифровой среды доверия.

Ключевые слова: информационная инфраструктура, доверенная сторона, цифровое пространство, среда доверия, цифровая трансформация

Для цитирования: Химченко А.И. Вопросы формирования цифровой среды доверия как структурного элемента в цифровизации государственного управления / А.И. Химченко // Правовое государство: теория и практика. – 2022. – № 3. – С. 159–164. DOI 10.33184/pravgos-2022.3.22.

Abstract. The article is devoted to the study of legal aspects of the digital environment of trust, identifying trends and problems related to the peculiarities of its formation in the context of digitalization of public administration. The emerging trend of increasing the role of remote communication requires a scientific understanding of the existing problems in order to create the digital environment of trust. In the process of digital transformation of public administration, there is a modification of forms and mechanisms of implementation, formation of new tools of interaction. The emerging trend of increasing the role of remote communication requires a scientific understanding of the problems in order to create the digital environment of trust. Purpose: to analyze the mechanisms for the implementation of trusted communications, to form proposals to stimulate the digital environment of trust. Research methods: analysis, systemic, abstraction, hypotheses, idealization, legal modeling, comparative legal. Results: the article identifies the development vectors of trusted communication mechanisms, analyzes the current situation and problematic issues and formulates proposals for the formation of the digital environment of trust.

Keywords: information infrastructure, trusted party, digital space, environment of trust, digital transformation

For citation: Khimchenko A.I. Issues of formation of the digital environment of trust as a structural element in the digitalization of public administration. *Pravovoe gosudarstvo: teoriya i praktika* = The Rule-of-Law State: Theory and Practice, 2022, no. 3, pp. 159–164. DOI 10.33184/pravgos-2022.3.22 (In Russian).

ВВЕДЕНИЕ

Государственное управление традиционно является одним из приоритетных объектов цифровизации. Принимая во внимание относительно недавний тренд на активную цифровизацию, а также отсутствие нормативного признания понятия «цифровая среда», следует отметить, что информатизация системы государственного управления продолжается длительное время, в процессе ее вопросы обеспечения доверенных коммуникаций всегда были актуальны.

Важным этапом деятельности по цифровизации государственного управления стало выделение в приоритеты государственной политики задачи по цифровизации экономики, выполнение программы «Цифровая экономика Российской Федерации» и национального проекта «Национальная программа «Цифровая экономика Российской Федерации»», а также специального федерального проекта «Цифровое государственное управление» в его структуре.

Активные процессы цифровизации трансформируют процесс функционирования государственных институтов, перестраивая привычные принципы взаимодействия и формируя новые.

Результатом активного внедрения информационно-коммуникационных и цифровых технологий в процессы государственного управления, среди которых предоставление услуг и функций, информационный обмен между участниками, надзор и контроль, осуществление судебных функций, стало увеличение удельной доли дистанционных технологий, электронного взаимодействия и усложнение специфики их функционирования.

В сложившихся условиях специфика, цели и задачи современных технологических преобразований определяют потребности в создании качественных отраслевых решений по формированию среды доверия субъектов цифрового взаимодействия.

Проблематика формирования среды доверия является признанной задачей и с определенного времени находится в фокусе государственного управления. Так, при разработке программы «Цифровая экономика Российской Федерации» среди вызовов цифровой трансформации была выделена проблема обеспечения доверия граждан к цифровой среде. При этом в научных работах формирование единой цифровой среды доверия признавалось и как условие формирования цифровой экономики [1].

Вместе с этим, согласно Указу Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской

Федерации на 2017–2030 годы»¹, в состав ключевых направлений развития российских информационных и коммуникационных технологий включены доверенные технологии электронной идентификации и аутентификации. Кроме того, формирование безопасной среды оборота достоверной информации признается Доктриной информационной безопасности РФ² в числе направлений реализации национальных интересов в информационной сфере.

Таким образом, формирование цифровой среды доверия является актуальной задачей в вопросе цифровизации государственного управления и отражает национальные интересы в информационной сфере.

ТЕКУЩАЯ СИТУАЦИЯ

В условиях отсутствия нормативного закрепления термина «цифровая среда», при этом исходя из логики понимания под ним условной совокупности информационных ресурсов и соответствующей инфраструктуры взаимодействия, очевидно, что в основе доверия лежит идентификация субъектов соответствующего цифрового взаимодействия, а также механизмы безопасного взаимодействия, возможности бесшовного применения информации во взаимодействии с внешней средой, реализации своих прав субъектами взаимодействия.

Технологии идентификации (ЕСИА, ЕБС, видеопоток). Технологии идентификации традиционно востребованы как при оказании традиционных государственных услуг и функций, так и при развитии структурных элементов цифровой экономики, реализации дистанционных форматов их функционирования. Актуальность тематики показывает и фокус внимания научного сообщества. Так, на необходимость создания системы правового регулирования доверенных коммуникаций обращал внимание В.Б. Наумов, выделяя ее как важный шаг в обеспечении безопасности идентификации субъектов правоотношений в цифровую эпоху [2, с. 75].

Проблематика удаленной идентификации длительное время не находила своего законодательного урегулирования. При этом разработка специального законодательства необходима для развития правового института идентификации [3, с. 139].

Поскольку ключевой риск идентификации состоит в возможности совершения юридически значимых действий под чужим

1 Собрание законодательства РФ. 2017. № 20, ст. 2901.

2 Собрание законодательства РФ. 2016. № 50, ст. 7074.

идентификатором помимо воли его законного владельца, приоритетным вопросом формирования среды доверия становится минимизация возможности осуществления таких действий [4, с. 27].

Кроме того, идентификация не должна быть исключительно атрибутом экономических отношений, стимулируя коммерческие цели развития, она должна быть связана и с гуманитарными и культурными задачами, в числе которых, как справедливо отмечают Т.А. Полякова и А.В. Минбалева, и стратегическая задача формирования «электронного пространства знаний», где связь объектов и субъектов и информационная безопасность последних играют значимую роль [5, с. 236].

В настоящее время основным механизмом, реализующим технологию удаленной идентификации, является Единая система идентификации и аутентификации (ЕСИА), реализованная в соответствии с Постановлением Правительства РФ от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»³.

Актуальной тенденцией развития института удаленной идентификации стало формирование механизмов на основе биометрических персональных данных.

Не имея возможности подробно остановиться на сущности биометрических персональных данных и специфике их оборота [5] проанализируем динамику развития реализуемых на их основе механизмов удаленной идентификации.

Так, положениями Федерального закона от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»⁴ были созданы правовые основы для реализации удаленной идентификации граждан по биометрическим персональным данным.

Ключевое значение в этом процессе имеет Единая биометрическая система (далее – ЕБС), которая в соответствии со ст. 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»⁵ является государственной информационной системой, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их

проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица. ЕБС функционирует в целях повышения качества и доступности услуг в электронном виде, при этом регулирование порядка функционирования ЕБС осуществляется специальными требованиями законодательства.

До определенного момента специфика использования финансовыми институтами ЕБС ограничивалась открытием счетов и кредитованием. Обязательным условием для работы с биометрическими данными при этом было наличие базовой банковской лицензии.

В дальнейшем Федеральным законом от 29 декабря 2020 г. № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»⁶ были внесены поправки, направленные на развитие биометрических технологий, а отдельными нормативными актами в течение 2021 г. производилась детальная настройка соответствующего механизма биометрической идентификации (например, Постановление Правительства РФ от 24 декабря 2021 г. № 2459 «О внесении изменений в Постановление Правительства Российской Федерации от 8 июня 2011 г. № 451»⁷, Постановление Правительства РФ от 23.10.2021 № 1815 «Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также случаев использования организациями, за исключением кредитных организаций, некредитных финансовых организаций, которые осуществляют указанные в части первой статьи 76.1 Федерального закона «О Центральном банке Российской Федерации (Банке России)» виды деятельности, субъектами национальной платежной системы, индивидуальными предпринимателями указанных информационных систем для идентификации либо идентификации и аутентификации физического лица, выразившего согласие на их проведение»⁸, Приказ Минцифры России от 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической

3 Собрание законодательства РФ. 2011. № 49 (ч. 5), ст. 7284.

4 Собрание законодательства РФ. 2018. № 1 (ч. 1), ст. 66.

5 Собрание законодательства РФ. 2018. № 1 (ч. 1), ст. 66.

6 Собрание законодательства РФ. 2021, № 1 (ч. 1), ст. 18.

7 Собрание законодательства РФ. 2022, № 1 (ч. 2), ст. 166.

8 Собрание законодательства РФ. 2021, № 44 (ч. 3), ст. 7423.

системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»⁹).

С 1 января 2021 г. с использованием ЕБС и ЕСИА разрешено проводить все банковские операции с юридическими и физическими лицами. Был усовершенствован процесс сбора биометрических персональных данных и осуществления дистанционной биометрической идентификации. Расширены возможности использования ЕБС при оказании государственных и муниципальных услуг, созданы регуляторные условия для реализации корпоративных биометрических систем.

Также следует отметить поиск возможностей расширения механизмов удаленной идентификации. Так, дорожная карта Банка России по развитию финансирования субъектов малого и среднего предпринимательства¹⁰ предусматривает рассмотрение возможности проведения банками процедуры удаленной идентификации клиента посредством технологий видеопотока с проведением пилотирования инициативы в регулятивной песочнице Банка России.

Анализ международного опыта показывает, что регуляторы отдельных стран – участниц Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) уже допускают проведение идентификации посредством применения технологий видеопотока.

Так, в соответствии с уведомлением № 2/2018¹¹ была подтверждена возможность реализации процедуры дистанционной идентификации посредством механизма видеоконференции. Кроме того, в соответствии с решением Федерального управления финансового надзора Германии (BaFin) применяется Циркуляр № 3/2017: «Процедуры

видеоидентификации»¹², регламентирующий применение видеоидентификации в практике финансовых организаций.

Обеспечение безопасного взаимодействия. Ключевой задачей формирования цифровой среды доверия становится необходимость обеспечения безопасности взаимодействия субъектов цифровой среды. В контексте развития инфраструктуры безопасного взаимодействия необходимо отметить Федеральный закон от 27 декабря 2019 г. № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»¹³, в соответствии с положениями которого были реализованы меры, направленные на повышение качества соответствующего взаимодействия посредством установления системы требований к удостоверяющим центрам, введение института «Доверенной третьей стороны», а также реализацию возможности использования «облачной» электронной подписи.

Вместе с тем вопрос организации безопасного взаимодействия содержит набор требующих к себе внимания моментов. Необходимо совершенствование механики выдачи и обращения электронной подписи (далее – ЭП) в целях минимизации возможности получения незаконного доступа к ключу проверки ЭП. Так, ситуацию осложняет отсутствие единого централизованного реестра усиленных квалифицированных электронных подписей (далее – УКЭП), выданных удостоверяющими центрами. Кроме того, отсутствует единый стандарт процесса выдачи УКЭП, не стандартизирован защищенный носитель УКЭП, протоколы проверки УКЭП дифференцированы как в зависимости от удостоверяющего центра, так и региона обращения.

Реализация прав субъектов. Не менее важным среди элементов, составляющих ландшафт цифровой среды доверия, является создание механизмов контроля предоставляемых данных субъектом взаимодействия на протяжении всего процесса дистанционного взаимодействия и их жизненного цикла в целом. На случай нарушения прав субъекта

9 Офиц. интернет-портал правовой информации [Электронный ресурс]. URL: <http://pravo.gov.ru> (дата обращения: 01.07.2022).

10 Дорожная карта Банка России по развитию финансирования субъектов малого и среднего предпринимательства: приказ Банка России от 13.09.2018 № ОД-2387 [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 15.07.2022).

11 Banco de Portugal: сайт [Электронный ресурс]. URL: https://www.bportugal.pt/sites/default/files/anexos/cartascirculares/329407737_5.docx.pdf (дата обращения: 01.07.2022).

12 Federal Financial Supervisory Authority: сайт [Электронный ресурс]. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html (дата обращения: 01.07.2022).

13 Собрание законодательства РФ. 2019. № 52 (ч. 21), ст. 7794.

в процессе взаимодействия логичным является наличие действующих правовых механизмов защиты прав субъектов взаимодействия, определение подсудности и подведомственности споров в указанной сфере. Кроме того, необходимо определение критериев и механизмов допустимости информации для подтверждения необходимых фактов (в качестве доказательств) в цифровой среде.

Действующее законодательство не содержит однозначного ответа на вопрос о порядке применения информации, формируемой в цифровой среде, в процессуальных отношениях. Так, ст. 71 ГПК РФ допускает использование документов и материалов, выполненных в форме цифровой записи, в качестве письменных доказательств. Вместе с тем в соответствии с п. 24 Постановления Пленума Верховного Суда РФ от 26 декабря 2017 г. № 57 в случае направления в суд электронных образов доказательств суд после возбуждения производства по делу может потребовать представления подлинников данных доказательств.

В указанной ситуации представляется целесообразным расширение инструментов доверенных коммуникаций посредством создания правового механизма «Доверенной стороны» для фиксации необходимой информации и фактов, законодательное определение соответствующего термина, закрепление статуса, прав и обязанностей, ответственности и регламентация правил работы с ней субъектов цифровой среды. Такое решение будет способствовать совершенствованию регуляторной среды, развитию инструментария доверенных коммуникаций и формированию рынка соответствующих технологических решений.

При этом, как уже было отмечено, в действующем законодательстве в целях обеспечения доверия при обмене данными и электронными документами уже создан институт «Доверенной третьей стороны», предназначенный для проверки электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ.

Кроме того, в решении Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125 реализован механизм службы доверенной третьей стороны интегрированной системы, определенный как совокупность сервисов доверенной третьей стороны государств-членов и Комиссии, обеспечивающих единое трансграничное пространство доверия при обмене электронными документами в интегрированной системе.

Пути решения

Для снижения возникающих факторов риска и формирования контура цифровой среды доверия необходим комплекс взаимосвязанных действий, среди которых правовые, технологические, методологические мероприятия.

1. Идентификация. Формирование цифровой среды доверия подразумевает совершенствование правовых механизмов идентификации. В действующем законодательстве необходимо определить состав субъектов в сфере идентификации, их правовой статус, права, обязанности и ответственность. Целесообразно также разработать дифференцированный подход к определению необходимого (применимого) уровня идентификации в зависимости от правоотношений (упрощенная, обычная, усиленная). Кроме того, необходимо определить ролевую модель в процессе идентификации таких потенциальных участников, как нерезиденты Российской Федерации, организации без создания юридического лица, индивидуальные предприниматели (ИП), адвокаты, иные лица, занимающиеся частной практикой и заинтересованные в удаленной идентификации.

2. Взаимодействие. В целях минимизации возможности неправомерного доступа к ключу проверки ЭП необходимо совершенствование механизма его выдачи и обращения. Целесообразно создание централизованного реестра УКЭП, стандартизация процесса выдачи УКЭП, стандартизация защищенного носителя УКЭП, обеспечение возможности использования физическими и юридическими лицами УКЭП, а также усиленной неквалифицированной ЭП ЕСИА (УНЭП ЕСИА). Указанные мероприятия целесообразно реализовывать при участии Банка России, с созданием соответствующего удостоверяющего центра Банка России.

3. Методологические. Необходима реализация технологических и методологических решений, среди которых разработка инструментов мониторинга, надлежащее выполнение сторонами (организациями, платформами) требований информационной безопасности идентификации клиентов. Вопросы разработки технических спецификаций, интеграции технических средств идентификации в информационную инфраструктуру организаций (цифровых платформ) целесообразно регламентировать.

Выводы

Формирование цифровой среды доверия отражает национальные интересы в информационной сфере, является сложной комплексной задачей и предполагает создание качественных правовых, технологических и методологических решений для функционирования эффективных и безопасных средств дистанционного взаимодействия.

Среди них развитие механизмов удаленной идентификации личности, расширение инструментов идентификации и аутентификации физических и юридических лиц, разработка сервисов доверенной стороны,

выработка условий признания результатов электронного взаимодействия.

Помимо создания безальтернативных условий для идентификации субъекта правоотношений в цифровой среде формирование цифровой среды доверия подразумевает выработку системы гарантий конфиденциальности, целостности и неизменности данных, а также обеспечение достоверности информации. Указанные решения находятся в фокусе вопросов информационной безопасности, что, в свою очередь, актуализирует проблематику форм и методов ее обеспечения на всех уровнях взаимодействия: от коммерческих компаний до государственных институтов.

Список источников

1. Терещенко Л.К. Единая цифровая среда доверия как условие формирования цифровой экономики / Л.К. Терещенко // Информационное право. – 2020. – № 4. – С. 12–15.
2. Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: монография / Т.А. Полякова и др.; под общ. ред. Т.А. Поляковой; Ин-т государства и права РАН. – Москва; Саратов: Амрит, 2022. – 332 с.
3. Наумов В.Б. Задача обеспечения тайны идентификации в информационном праве / В.Б. Наумов // Мониторинг правоприменения. – 2019. – № 3 (32). – С. 70–75.
4. Наумов В. Цифровая среда доверия / В. Наумов, Е. Авакян, А. Чубурков, Р. Янковский, С. Белова, М. Тевс, Э. Махносов, В. Рыбалко // Закон. – 2019. – № 9. – С. 25–38.
5. Камалова Г.Г. Биометрические персональные данные: определение и сущность / Г.Г. Камалова // Информационное право. – 2016. – № 3. – С. 8–12.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Химченко Алексей Игоревич – кандидат юридических наук, старший преподаватель кафедры информационного права и цифровых технологий Московского государственного юридического университета им. О.Е. Кутафина (МГЮА).

INFORMATION ABOUT THE AUTHOR

Khimchenko Aleksey Igorevich – Candidate of Sciences (Law), Senior Lecturer of the Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL).

Статья поступила в редакцию 06.06.2022; одобрена после рецензирования 10.07.2022; принята к публикации 19.08.2022. The article was submitted 06.06.2022; approved after reviewing 10.07.2022; accepted for publication 19.08.2022.

REFERENCES

1. Tereshchenko L.K. Unified digital environment of trust as a condition for the formation of the digital economy. *Informacionnoe pravo = Information Law*, 2020, no. 4, pp. 12–15. (In Russian).
2. Polyakova T.A., Minbaleev A.V., Naumov V.B., Zharova A.K., Boychenko I.S., Berman A.M.; Polyakova T.A. (ed.). *Formirovanie sistemy pravovogo regulirovaniya obespecheniya informacionnoj bezopasnosti v usloviyah bol'shikh vyzovov v global'nom informacionnom obshchestve* [Formation of the system of legal regulation of information security in the face of great challenges in the global information society]. Moscow, Saratov, Amirit Publ., 2022. 332 p.
3. Naumov V.B. The task of ensuring the secrecy of identification in information technology law. *Monitoring pravoprimeneniya = Monitoring of Law Enforcement*, 2019, no. 3 (32), pp. 70–75. (In Russian).
4. Naumov V., Avakyan E., Chuburkov A., Yankovsky R., Belova S., Tevs M., Makhnonosov E., Rybalko V. Digital Environment of Trust. *Zakon = Law*, 2019, no. 9, pp. 25–38. (In Russian).
5. Kamalova G.G. Biometric personal data: definition and nature. *Informacionnoe pravo = Information Law*, 2016, no. 3, pp. 8–12. (In Russian).