

Проблема цифровой идентификации личности в Российской Федерации и Европейском Союзе

Аннотация. Проблемы цифровой идентификации личности актуализировались в связи с пандемией COVID-19, но в то же время цифровая идентификация является необходимым условием устойчивого развития стран в цифровом обществе. Применение информационных технологий в целях идентификации физических лиц регламентируется правовыми нормами. В данной статье анализируется опыт решения проблем цифровой идентификации, обеспечения защиты биометрических персональных данных в Российской Федерации и Европейском Союзе. Рассматриваются формы верификации, цифрового подтверждения личности (идентификации) средствами аутентификации. В Европейском Союзе принят Регламент eIDAS электронной идентификации, определяющий требования и критерии к техническим средствам защиты информации, генерации электронных подписей. В ходе исследования выявлено, что в Эстонии наиболее развитая национальная система идентификационных карт (ID-карт) в мире. Рассмотрены проблемы и предложены меры нормативного регулирования процедуры цифровой идентификации личности, формирования цифрового профиля.

Ключевые слова: цифровая идентификация, личность, персональные данные, правовое регулирование информационных технологий и защиты информации.

DOI: 10.17803/2311-5998.2022.89.1.017-029

M. A. EGOROVA,

Dr. Sci. (Law), Professor, Head of the International Cooperation Department of Kutafin Moscow State Law University (MSAL), Expert of the Center for scientific and expert analysis of the Institute of Scientific and expert-analytical activity of the Russian State Academy of Intellectual Property, Expert of the Russian Academy of Sciences
maegorova@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

The problem of digital identity identification in the Russian Federation and the European Union

Abstract. Problems of digital identification have become relevant due to the COVID-19 pandemic, but at the same time, digital identification is a prerequisite for the sustainable development of countries in a digital society. Law regulates the use of information technology in identification of individuals. This article analyzes the experience of solving digital identification problems,



**Мария Александровна
ЕГОРОВА,**

доктор юридических наук, профессор, начальник Управления международного сотрудничества, эксперт Центра научной и экспертной аналитики Международного центра компетенций «АйПи» Российской государственной академии интеллектуальной собственности (РГАИС), эксперт РАН
maegorova@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

© М. А. Егорова, 2022

ensuring the protection of biometric personal data in the Russian Federation and the European Union. Forms of verification, digital identity authentication (identification) by means of authentication are considered in this article as well. The European Union has adopted the eIDAS Electronic Identification Regulation, which defines the requirements and criteria for technical means of protecting information and generating electronic signatures. The study revealed that Estonia has the most developed national identification card system (ID-cards) in the world. The article considers the problems related to the issue and proposes regulatory measures aimed at the digital identification procedure and formation of a digital profile.

Keywords: *digital identification, personality, personal data, legal regulation of information technology and information protection.*

Развитие современного информационного общества предполагает возможность реализации публичных, гражданских, процессуальных и иных правоотношений в цифровой среде. Одним из наиболее важных вопросов, который предстоит решить законодателю, — идентификация пользователя в цифровом пространстве¹. Цифровая идентификация — это набор технологий и интеллектуальных устройств, позволяющих верифицировать личность по цифровой информации: биометрическим данным (отпечаткам пальцев, скану лица, сетчатке глаза), цифровым паспортам или ID, паролям, ПИН-кодам, QR-кодам.

Если ранее все правоотношения возникали и прекращались в реальном мире и было достаточно документа, удостоверяющего личность, и личного присутствия, то теперь подобные документы непригодны для подтверждения личности в интернет-пространстве, так как личное присутствие заменяется виртуальным².

Системы цифровой идентификации используют электронные средства для подтверждения официальной личности человека в онлайн-овой (цифровой) среде. Цифрой ID используется для отслеживания цифрового следа индивида. Цифровые идентификационные программы позволяют аутентифицировать личность, т.е. определить, кем она является, посредством цифровых каналов, включая мобильные интерфейсы, интернет-браузеры или центральную систему интернет-аутентификации.

Форма нового подтверждения личности может быть различной: от электронного удостоверения, которое заменяет паспорт и иные документы, до приложения, установленного на смартфоне. Однако в любом случае независимо от формы идентификация в виртуальном пространстве связана с множеством рисков, возникающих в контексте информационной безопасности. Во-первых, существует вероятность идентификации в виртуальном пространстве лиц, использующих чужие данные. Во-вторых, особенно остро стоит проблема хранения и защиты

¹ Лучков О. А. Идентификация субъектов в цифровом пространстве: несколько правовых проблем // Правопорядок: история, теория, практика. 2019. № 1 (20). С. 6—9.

² Основные тренды развития цифровой экономики в финансовой сфере. Правовые аспекты регулирования и практического применения / под ред. А. Г. Аксакова ; Государственная Дума РФ. М., 2019. 161 с.

данных. Можно представить последствия утечки из огромного массива информации, где будут консолидированы все данные о гражданине.

Система идентификации в Российской Федерации регулируется Федеральными законами «Об информации, информационных технологиях и о защите информации»³ и «О государственной дактилоскопической регистрации в Российской Федерации»⁴, а также Порядком проведения идентификации личности человека по пальцам⁵.

Цифровая идентификация личности — это в значительной мере технические и организационно-технические методы, связанные с идентификацией и аутентификацией, следовательно, необходимы требования, аналогично разработанные и утвержденные для защиты персональных данных.

Единая система идентификации и аутентификации — федеральная государственная информационная система, порядок использования которой устанавливается Правительством РФ, обеспечивающая в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Правом внесения сведений, в том числе биометрических данных, в ЕСИА обладают государственные органы, банки и иные организации.

В соответствии с постановлением Правительства РФ от 28.11.2011 № 977⁶ ЕСИА должна обеспечивать санкционированный доступ участников информационного взаимодействия (заявителей и должностных лиц органов государственной власти) к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах.

Разработчики государственных сайтов, порталов и прочих веб-приложений могут предоставить своим пользователям возможность входить в систему, используя учетную запись ЕСИА. Это избавляет разработчиков от необходимости

³ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // URL: http://www.consultant.ru/document/cons_doc_law_61798/ (дата обращения: 05.10.2021).

⁴ Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» (с изм. и доп.) // URL: <https://base.garant.ru/179140/> (дата обращения: 11.08.2021).

⁵ Приказ МВД России от 19.06.2018 № 384 «Об утверждении Порядка проведения идентификации личности человека по отпечаткам пальцев (ладоней) рук в режиме реального времени и Перечня категорий лиц, в отношении которых обязательная государственная дактилоскопическая регистрация не проводится в случае идентификации их личности в результате проверки по отпечаткам пальцев (ладоней) рук в режиме реального времени» // URL: <https://юфот.мвд.рф/document/14197417> (дата обращения: 11.08.2021).

⁶ Постановление Правительства РФ от 28.11.2011 № 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»» // URL: http://www.consultant.ru/document/cons_doc_law_122455/ (дата обращения: 05.10.2021).



делать собственное хранилище учетных записей, обеспечивать безопасность хранения паролей, разрабатывать механизмы регистрации, аутентификации пользователей, поддерживать их в рабочем состоянии.

Действия по идентификации и (или) аутентификации физического лица с использованием единой биометрической системы и единой системы идентификации и аутентификации приравниваются к действиям по проверке документов, удостоверяющих личность такого физического лица.

Таким образом, в настоящее время для того, чтобы воспользоваться услугами в электронном виде, необходимо авторизоваться через учетную запись, созданную на портале Госуслуг. При этом существуют две степени верификации: простая электронная подпись (для ее получения достаточно предъявить в МФЦ документ, удостоверяющий личность и СНИЛС) и квалифицированная электронная подпись, которую можно получить в органах ФНС или аккредитованных удостоверяющих центрах.

В настоящее время в России сбор данных в Единую биометрическую систему (ЕБС) осуществляется только при личном визите человека в отделение банка. Считаем возможным рассмотрение вопроса о дистанционной регистрации в ЕБС.

Большинство граждан Российской Федерации используют простую электронную подпись и авторизуются с помощью логина и пароля. Следует отметить, что авторизация через ЕСИА не имеет глобального характера, т.е. такая авторизация не является универсальным способом предъявления документа перед неограниченным числом лиц даже на территории Российской Федерации.

Также доступ исключительно с помощью логина и пароля не может быть признан достаточно надежным. Более рациональным выглядит использование двухфакторной аутентификации, например с помощью ввода постоянного пароля пользователя, а также повторного подтверждения личности с помощью ввода одноразового пароля, пришедшего по SMS.

Если же рассматривать более глобальное использование идентификации и аутентификации, то необходимо повышать степень защиты с помощью использования биометрических данных⁷.

Даже криптографический метод шифрования данных не может дать полную защиту цифрового образа личности. Любой пароль может быть скомпрометирован (взломан, утерян). Решить проблему запоминания пароля и отчуждения его от человека способна только биометрия⁸.

Внедрение в базу данных единой системы биометрических данных потребует усиления всех возможных методов защиты информации, так как при их утечке может быть нанесен огромный урон. Актуальность требования к безопасному хранению данных продиктована тем, что доступ к единой системе имеют не только государственные органы, но и иные лица, в том числе банки. Информационное

⁷ Сазонова М. Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть // URL: <https://www.garant.ru/news/1460152/> (дата обращения: 02.10.2021).

⁸ Журба А. Ученые Омского «политеха» создали технологию дистанционной идентификации личности // URL: <https://omsk.mk.ru/science/2021/01/15/uchenye-omskogo-politekha-sozdali-tehnologiyu-distancionnoy-identifikacii-lichnosti.html> (дата обращения: 10.08.2021).

пространство периодически сотрясают новости о крупных утечках из баз данных клиентов банков.

Еще одной проблемой использования системы идентификации и аутентификации в цифровой среде является определение дееспособности пользователя. База данных судебных решений о признании гражданина ограничено дееспособным / недееспособным, оператором которой был Росреестр, не является на 100 % актуальной. В 2020 г. Федеральным законом «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам, связанным с распоряжением средствами материнского (семейного) капитала»⁹ установлено, что сведения об ограничении дееспособности гражданина или о признании гражданина недееспособным теперь хранятся в Единой государственной информационной системе социального обеспечения. Однако на признание гражданина недееспособным, внесение соответствующих данных необходимо время. В этом временном промежутке недееспособный гражданин может вполне успешно совершать юридически значимые действия в цифровом пространстве. Также встает вопрос об актуальности внесенных в систему данных.

Одной из задач эффективной идентификации и аутентификации является создание единой системы доступа ко всем государственным услугам. Для этого, в свою очередь, необходимо консолидировать все данные, которые находятся в разных ведомствах (ПФР, загсе, Росреестре и т.п.) в одну базу. С одной стороны, пользователь сможет получать любые государственные услуги в режиме «одного окна» (в рамках обращения к единому сайту). С другой стороны, уполномоченные лица смогут получать всеобъемлющие данные о конкретном лице.

В 2019 г. в проекте федерального закона № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)»¹⁰ было предложено ввести понятие цифрового профиля лица как совокупности сведений о гражданах и юридических лицах, которые находятся в различных государственных информационных системах. Предполагалось создание национальной системы управления данными (НСУД). Однако данный законопроект так и не был одобрен Государственной Думой.

В последнее время расширяются форматы электронных рыночных и торговых отношений, удаленной трудовой деятельности и всех видов обучения с использованием цифровых технологий связи, в 2020 г. внесены изменения в Трудовой кодекс РФ, следовательно, проблемы идентификации личности становятся особенно важными. При этом верификация и аутентификация должны быть выполнены с высокой степенью гарантии, уникальными, устанавливаться только с согласия индивида, защищать конфиденциальность и обеспечивать защиту персональных данных. Проблемой является то, что граница между основной и

⁹ Федеральный закон от 01.03.2020 № 35-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам, связанным с распоряжением средствами материнского (семейного) капитала» // URL: http://www.consultant.ru/document/cons_doc_LAW_346665/ (дата обращения: 04.10.2021).

¹⁰ См.: Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») // URL: <https://sozd.duma.gov.ru/bill/747513-7>.



расширенной версией цифрового идентификатора весьма размыта, поэтому даже базовый идентификатор можно использовать для связи с другими базами данных.

Одним из обсуждаемых вопросов становится введение цифровых профилей личности, цифровых паспортов здоровья, электронных паспортов, но основными проблемами этого процесса являются обеспечение кибербезопасности и высокой защиты в информационных системах, интеграция с криптокабинетами МФЦ.

Необходимо отметить, что в зарубежных странах также остро стоит вопрос перехода личности в цифровое пространство, в связи с чем разработаны соответствующие нормативные акты.

В США нет единого основного законодательства о защите данных. США отстают от ЕС в отношении защиты конфиденциальности.

В странах Евросоюза с 01.07.2016 начал работать регламент eIDAS (electronic ID entification, Authentication and trust Services) об электронной идентификации и доверенных услугах¹¹. Обязательное взаимное признание электронных идентификаторов странами Евросоюза действует с 29.09.2018. В каждой стране свои стандарты идентификации и электронной цифровой подписи (ЭЦП), но eIDAS представляет собой набор «лучших практик», который гарантирует совместимость ЭЦП на европейском уровне, потому что все публичные организации Евросоюза обязаны признавать квалифицированные ЭЦП из других стран.

eIDAS устанавливает единый стандарт, которому должно соответствовать аппаратное и программное обеспечение для генерации цифровых подписей. Все токены проходят обязательную сертификацию. Для физических лиц таким токеном (идентификатором) может служить, например, электронный паспорт или смартфон, а для организаций — смарт-карты, USB-токены и иные устройства¹².

В то же время в Евросоюзе невозможно одновременно «ввести» некую единую систему идентификации, поскольку каждая страна — член ЕС является суверенным государством. Акты вторичного законодательства ЕС, прежде всего директивы и регламенты, принятие которых направлено на создание основополагающего нормативно-правового фундамента взаимодействия государств-членов, не могут не учитывать различия, в том числе в плане технологического развития стран — членов ЕС применительно к системам и средствам идентификации.

С одной стороны, Регламент eIDAS исходит из того, что государства-члены остаются свободными в использовании или внедрении средств для целей электронной идентификации для доступа к онлайн-услугам; обладают возможностью решать, следует ли привлекать частный сектор к предоставлению такого рода средств; не обязаны уведомлять Европейскую комиссию ЕС о своих электронных системах идентификации.

С другой стороны, необходимо принимать во внимание, что в большинстве случаев граждане ЕС не могут использовать свои электронные идентификационные данные, полученные в стране — члене ЕС, для аутентификации в другом

¹¹ 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 (дата обращения: 06.10.2021).

¹² European Comissioin. eIDAS Regulation // URL: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation> (дата обращения: 08.08.2021).

государстве — члене ЕС, поскольку национальные электронные идентификационные системы и средства их страны не признают иные системы и средства идентификации других государств — членов ЕС¹³. Соответственно, ключевым принципом, из которого исходит Регламент eIDAS, является взаимное признание государствами — членами ЕС электронных систем и средств идентификации, существующих в государствах — членах ЕС.

Страны — члены Евросоюза вправе самостоятельно решать вопрос о том, разрешают ли они использование электронных средств идентификации для онлайн-доступа в своей юрисдикции к своим общедоступным услугам, если уровень доверия электронных средств идентификации другой страны — члена ЕС ниже уровня доверия, предусмотренного Регламентом eIDAS, или равен ему. Этот подход подчеркивает, что управление идентичностью в цифровой среде базируется на децентрализованной идентификации, когда лица (физические/юридические) имеют возможность создавать и контролировать свою личность, не полагаясь на какую-либо централизованную власть.

EIDAS обеспечивает: правовую определенность за пределами национальных границ, единую нормативную среду для беспрепятственного международного признания eID и трастовых услуг.

EIDAS повышает: доверие; безопасность; удобство (онлайн) для правительства, бизнеса и потребителей¹⁴.

Услуги идентификации помогают проверить личность физических и юридических лиц, взаимодействующих в Интернете, а также подлинность удостоверяющих документов, предъявленных в электронной форме. В этой связи на внутреннем рынке Евросоюза при заключении сделок в электронной форме (в том числе трансграничных), согласно Регламенту eIDAS используются следующие средства электронной идентификации: электронные подписи (Electronic signatures), электронная печать (Electronic seals), штамп времени (Timestamps), электронная зарегистрированная служба доставки (Electronic registered delivery), аутентификация сайта (Website authentication).

Европейский совет (European Council) призывает к разработке общеевропейской структуры для безопасной общественной электронной идентификации (e-ID), включающей функционально совместимые цифровые подписи, чтобы предоставить гражданам ЕС контроль над своей онлайн-идентичностью и данными, а также обеспечить доступ к общедоступным и частным данным, трансграничным цифровым услугам.

В настоящее время большинство стран — членов ЕС уже обменялись уведомлениями о тех национальных системах идентификации, которые дают возможность получить широкий трансграничный доступ к услугам общего пользования в рамках Евросоюза¹⁵.

¹³ Касенова М. Системы цифровой идентификации лиц: будущее и реальность // Интернет изнутри. Информационный сборник. 2020 // URL: <https://internetinside.ru/sistemy-cifrovoy-identifikacii-lic-b/>.

¹⁴ Building a Trusted and Secure European Digital Identity — Brochure // URL: <https://digital-strategy.ec.europa.eu/en/library/building-trusted-and-secure-european-digital-identity-brochure> (дата обращения: 05.10.2021).

¹⁵ Altmann P., Rissanen E. Self-Sovereign Digital Identity on the European Blockchain Services Infrastructure. September 2020. DOI: 10.13140/RG.2.2.30892.49281.



Однако есть и исключения, которые свидетельствуют о существующих сложностях внедрения системы идентификации. Так, швейцарский парламент принял Федеральный закон «О цифровой идентификации» (E-ID-Gesetz), который был отменен проведенным 07.03.2021 референдумом¹⁶.

В отличие от многих других европейских стран, в Швейцарии пока нет сертифицированных государством методов проверки цифровой идентичности жителя страны (eID). При этом eID не является цифровым паспортом. Это единый логин, который позволяет пользоваться цифровыми госуслугами.

Принятый парламентом в 2019 г. закон предусматривал усеченную роль государства в создании системы идентификации. На государство возлагалась обязанность создать лишь базовую инфраструктуру.

Работу по организации системы цифровой идентификации личности в сети предполагалось поручить частным компаниям в сотрудничестве с кантональными и муниципальными органами власти, которые выдавали бы электронные удостоверения личности. Для предотвращения злоупотреблений создавался независимый орган по сертификации и надзору за такими частными компаниями.

Отмена закона была связана с тем, что подверглась критике большая роль частных компаний в аккумулировании персональных данных. Гражданам более безопасным видится создание системы, полностью контролируемой государством.

Кроме того, если государство будет единственным источником сертифицированной цифровой идентичности, то этот опыт поможет ему в будущем решить вопрос организации в стране надежной системы электронного голосования.

Одним из передовых государств в Евросоюзе в сфере цифровой идентификации является Эстония¹⁷. В отличие от жителей многих других стран, у каждого эстонца, независимо от его местонахождения, есть цифровая идентификация, выданная государством. Благодаря этому Эстония на годы опередила страны, которые все еще пытаются разработать способы аутентификации людей без физического контакта.

В Эстонии существует самая развитая национальная система идентификационных карт (ID-карт) в мире. Обязательная национальная карта (national ID-card) — это не только официальное удостоверение личности с фотографией, но и цифровой доступ ко всем защищенным электронным услугам Эстонии. Чип на карте содержит встроенные файлы, и посредством 384-битного шифрования с открытым ключом ECC его можно использовать в качестве окончательного подтверждения личности в электронной среде.

В Эстонии каждый человек может поставить цифровую подпись с помощью своей ID-карты, Mobile-ID или Smart-ID, чтобы безопасно идентифицировать себя и пользоваться электронными услугами. Вот несколько примеров их регулярного использования в Эстонии: официальный туристический ID для граждан Эстонии, путешествующих в пределах ЕС; карта государственного медицинского

¹⁶ Цифровая идентификация и проблема безопасности данных в Швейцарии / Швейцарская национальная теле- и радиокорпорация SRG SSR // URL: <https://www.swissinfo.ch/rus/politics/цифровая-идентификация-и-проблема-безопасности-данных-в-швейцарии/46321694> (дата обращения: 08.08.2021).

¹⁷ ID-Card // URL: <https://e-estonia.com/solutions/e-identity/> (дата обращения: 04.10.2021).

страхования; подтверждение личности при входе в банковский счет; для цифровых подписей; для i-голосования; для проверки медицинских карт; для подачи налоговых претензий и т.д.

Удостоверение личности, или ID-карта, является обязательным документом, удостоверяющим личность гражданина Эстонии и постоянно проживающего в Эстонии гражданина Европейского Союза. Кроме обычного удостоверения личности, ID-карту можно использовать и для личной идентификации в электронной среде, а также для цифровой подписи. В пределах Европейского Союза граждане Эстонии могут использовать ID-карту и в качестве рейсового документа. Дигитальное удостоверение личности (диги-ID) — это аналог электронной части ID-карты. Дигитальное удостоверение личности невозможно использовать для визуальной идентификации личности, так как на карту не наносится фото пользователя. Диги-ID можно использовать только в электронной среде для идентификации личности и цифровой подписи.

Мобильный ID (mobii-ID) — аналог диги-ID, позволяющий при помощи sim-карты мобильного телефона использовать электронные услуги, доступные обладателям ID-карты или диги-ID. При помощи мобильного ID можно идентифицировать личность в электронной среде и ставить цифровую подпись¹⁸.

Системы цифровой идентификации могут включать в себя компонент, позволяющий переносить удостоверение личности. Переносимая идентификация означает, что учетные данные цифрового удостоверения личности могут использоваться для подтверждения официальной личности для новых отношений с клиентами в несвязанных частных сектор или государственные учреждения, без необходимости получать и проверять личные данные, и регулярно проводить идентификацию/проверку клиентов. Переносимость может поддерживаться различными архитектурами и протоколами цифровых удостоверений. В Европе Регламент eIDAS обеспечивает основу для перекрестного признания систем цифровой идентификации.

Разнообразие существующих способов идентификации в Эстонии связано в том числе с тем, что в 2017 г. граждане в массовом порядке вынуждены были менять электронное удостоверение личности (следовательно, на какое-то время остались без возможности функционирования в цифровой среде) в связи с бракованными встроенными чипами¹⁹. Такие ситуации свидетельствуют об уязвимости системы электронной идентификации и наличия множества рисков.

Проверка личности имеет решающее значение также и для экономики²⁰.

¹⁸ Цифровые документы: ID-карта, цифровой-ID, карта вида на жительство, цифровой-ID э-резидента / Департамент государственной инфосистемы // URL: <https://www.id.ee/ru/artikkel/czifrovye-dokumenty-id-karta-czifrovoj-id-karta-vida-na-zhitelstvo-czifrovoj-id-e-rezidenta/> (дата обращения: 08.08.2021).

¹⁹ Эстония заблокировала электронные паспорта из-за бракованных чипов // URL: <https://news.finance.ua/ru/news/-/414166/estoniya-zablokirovala-elektronnye-pasporta-iz-za-brakovannyh-chipov> (дата обращения: 08.08.2021).

²⁰ Guidance on Digital Identity // FATF. Paris, March, 2020. 107 p. URL: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-on-digital-identity.pdf> (дата обращения: 06.10.2021).



Отсутствие надежной, простой в использовании цифровой идентификации и проверки имеет обременительные, сложные и дорогостоящие последствия для всех предприятий, особенно для стартапов и малых предприятий²¹.

Органам ПОД/ФТ следует рассмотреть вопрос о принятии механизмов для расширения диалога и сотрудничества с соответствующими заинтересованными сторонами из частного сектора, включая регулируемые организации и поставщиков услуг цифрового удостоверения личности, для определения ключевых возможностей, рисков и мер по снижению рисков, связанных с идентификацией. Механизмы могут включать нормативный подход «песочницы» для обеспечения контролируемой среды для проверки того, как системы цифровой идентификации взаимодействуют с национальными законами и нормативными актами в области ПОД/ФТ.

Международная организация по стандартизации (ISO) в настоящее время занимается разработкой глобальных стандартов идентификации физических лиц для финансовых услуг, в том числе в цифровом контексте.

Европейский Союз — первый и единственный регион в мире, где цифровое удостоверение личности и верификация обеспечиваются надежно и имеют юридическую силу. Европа прошла непростой путь к цифровой идентификации. По отчету Еврокомиссии, контент идентификации должен быть универсальным, преодолеть различия национальных правовых режимов и технических стандартов²². Организационные и технические инфраструктуры разрабатываются для определения, обозначения и администрирования идентичности, связанной с конкретными группами людей. Эти инфраструктуры представляют собой системы управления идентификацией, необходимые для эффективной и безопасной обработки данных, связанных с пользователями.

Во всех государствах — членах ЕС реализуются несколько инициатив по внедрению электронных идентификаторов (eID) для государственных услуг. Электронное удостоверение личности (eID) отличается от цифрового удостоверения личности. Электронное удостоверение личности — это средство, с помощью которого люди могут электронным образом доказать, что они те, кем они себя называют, и таким образом получить доступ к контенту государственных услуг. Работа с электронным удостоверением личности и персональными данными требует соответствующего регулирования обработки, хранения и использования данных.

Европейская цифровая идентификация будет доступна гражданам, резидентам и предприятиям ЕС, которые хотят идентифицировать себя или предоставить подтверждение определенной личной информации. Идентификатор eID можно использовать для получения государственных и частных услуг как онлайн, так и офлайн на всей территории ЕС. Каждый гражданин и житель Евросоюза сможет пользоваться личным цифровым кошельком. Цифровая идентификация признается в любой стране ЕС²³.

²¹ Echikson W. Europe's digital identification opportunity. Centre for European Policy Studies (CEPS). 2019. 37 p. // URL: https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity.pdf (дата обращения: 05.10.2021).

²² Electronic Identities — a brief introduction // URL: https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf (дата обращения: 05.10.2021).

²³ Digital Identity for all Europeans // URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (дата обращения: 06.10.2021).

Меры по цифровой идентификации всех граждан ЕС финансируются пакетом ЕС по восстановлению после коронавируса. European Digital Identity Wallet, предложенный исполнительной комиссией ЕС, представляет собой приложение для смартфонов, которое позволит пользователям хранить электронные удостоверения личности и другие официальные документы, такие как водительские права, медицинские рецепты и школьные аттестаты, подавать заявление в университет, осуществлять регистрацию в отеле и др.²⁴.

Еврокомиссия предложила государствам-членам подготовить к сентябрю 2022 г. общий набор инструментов, включая техническую архитектуру, стандарты и руководящие принципы (руководства, регламенты). Необходим скоординированный подход к цифровой идентификации на уровне ЕС, чтобы позволить гражданам и бизнесу воспользоваться возможностями, которые предлагает единый цифровой рынок для предоставления услуг и доступа к ним через границы²⁵.

Подводя итог, можно сделать следующие выводы:

1. Целесообразно учитывать передовой опыт ЕС в сфере цифровых удостоверений личности, создавать как на национальном, так и на международном уровне правовые рамки, позволяющие повысить гибкость, эффективность и функциональность систем цифровой идентификации.
2. Необходимо создать единую базу данных для точной идентификации личности в цифровом пространстве и возможности граждан действовать в цифровой среде в режиме «одного окна». При этом такая база должна быть защищена от любых утечек данных.
3. Целесообразно усилить защиту данных путем проведения двухфакторной идентификации, а в последующем внедрения биометрии.
4. Рационально предусмотреть вариативность подтверждения личности в интернет-пространстве (электронное удостоверение, электронная подпись, биометрические данные, абонентский номер и т.п.). В случае потери контроля лица над одним из способов идентификации и аутентификации всегда можно будет восстановить доступ с помощью иного способа.
5. Необходимо постепенное расширение возможности использования цифровой идентификации не только для получения государственных услуг, но и для регулирования правоотношений между физическими и юридическими лицами.
6. Нередко персональные данные становятся доступны, соответственно, необходимы более четкие механизмы технического, организационного и организационно-технического характера для защиты персональной информации и ответственности за их несанкционированное распространение, в том числе в корыстных и мошеннических целях.

²⁴ European Union Unveils Plans For A Digital Identity Wallet Funded By The EU Post-Covid Recovery Package To Digitize All European Citizens // URL: <https://www.nowtheendbegins.com/european-union-unveils-plans-digital-identity-wallet-funded-by-eu-post-covid-recovery-package-digitize-all-european-citizens-great-reset/> (дата обращения: 04.10.2021) ; First glimpse of EU's new 'digital identity wallet' // URL: <https://euobserver.com/news/152042> (дата обращения: 06.10.2021).

²⁵ Blockchain and digital identity. Thematic Report // URL: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf (дата обращения: 05.10.2021).



7. Представляется, что безопасность цифровых технологий является ключевым фактором, обеспечивающим доверие к ним. Эффективное осуществление цифровой идентификации личности является той задачей, решение которой поможет достигнуть определенного уровня безопасности, а следовательно, доверия граждан к новым технологиям.
8. Инструменты и технологии цифровой идентификации должны разрабатываться с учетом прав человека, свободы личности и передвижения, защиты персональных данных, морально-этических принципов. Цифровые технологии дают новые средства для поддержки, защиты и осуществления прав человека, но они также могут использоваться для подавления, ограничения или нарушения этих прав.

БИБЛИОГРАФИЯ

1. Журба А. Ученые Омского «политеха» создали технологию дистанционной идентификации личности // URL: <https://omsk.mk.ru/science/2021/01/15/uchenye-omskogo-politekha-sozdali-tekhnologiyu-distancionnoy-identifikacii-lichnosti.html> (дата обращения: 10.08.2021).
2. Касенова М. Системы цифровой идентификации лиц: будущее и реальность // Интернет изнутри : информационный сборник. — 2020. — URL: <https://internetinside.ru/sistemy-cifrovoy-identifikacii-lic-b/>.
3. Основные тренды развития цифровой экономики в финансовой сфере. Правовые аспекты регулирования и практического применения / под ред. А. Г. Аксакова ; Государственная Дума РФ. — М., 2019. — 161 с.
4. Пучков О. А. Идентификация субъектов в цифровом пространстве: несколько правовых проблем // Правопорядок: история, теория, практика — 2019. — № 1 (20). — С. 6—9.
5. Сазонова М. Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть // URL: <https://www.garant.ru/news/1460152/> (дата обращения: 02.10.2021).
6. Цифровая идентификация и проблема безопасности данных в Швейцарии / Швейцарская национальная теле- и радиокomпании SRG SSR // URL: <https://www.swissinfo.ch/rus/politics/цифровая-идентификация-и-проблема-безопасности-данных-в-швейцарии/46321694> (дата обращения: 08.08.2021).
7. Эстония заблокировала электронные паспорта из-за бракованных чипов // URL: <https://news.finance.ua/ru/news/-/414166/estoniya-zablokirovala-elektronnye-pasporta-iz-za-brakovannyh-chipov> (дата обращения: 08.08.2021).
8. Altmann P., Rissanen E. Self-Sovereign Digital Identity on the European Blockchain Services Infrastructure. September 2020 // URL: file:///c:/users/1/appdata/local/temp/ssi_ebsi.pdf. — doi: 10.13140/RG.2.2.30892.49281/ (дата обращения: 02.10.2021).
9. Blockchain and digital identity. Thematic Report // URL: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf (дата обращения: 05.10.2021).

10. Building a Trusted and Secure European Digital Identity — Brochure // URL: <https://digital-strategy.ec.europa.eu/en/library/building-trusted-and-secure-european-digital-identity-brochure> (дата обращения: 05.10.2021).
11. Digital Identity for all Europeans // URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (дата обращения: 06.10.2021).
12. *Echikson W.* Europe's digital identification opportunity /. Centre for European Policy Studies (CEPS). — 2019. — 37 p. // URL: https://www.ceps.eu/wp-content/uploads/2020/06/TFR_Europe-Digital-Identification-Opportunity.pdf (дата обращения: 05.10.2021).
13. Electronic Identities — a brief introduction. // URL: https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf (дата обращения: 05.10.2021).
14. European Union Unveils Plans for a Digital Identity Wallet Funded by the EU Post-Covid Recovery Package to Digitize all European Citizens // URL: <https://www.nowtheendbegins.com/european-union-unveils-plans-digital-identity-wallet-funded-by-eu-post-covid-recovery-package-digitize-all-european-citizens-great-reset/> (дата обращения: 04.10.2021).
15. First glimpse of EU's new 'digital identity wallet'. // URL: <https://euobserver.com/news/152042> (дата обращения: 06.10.2021).
16. Guidance on Digital Identity,. — FATF,. — Paris., March, 2020. — 107 p. — URL: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf> (дата обращения: 06.10.2021).