DOI 10.37882/2223-2974.2025.11.02

ПОНЯТИЕ И ПРАВОВАЯ ПРИРОДА ЦИФРОВОЙ ИДЕНТИФИКАЦИИ В ЭКОНОМИЧЕСКИХ ОТНОШЕНИЯХ

THE CONCEPT AND LEGAL NATURE OF DIGITAL IDENTIFICATION IN ECONOMIC RELATIONS

R. Gazizullin

Summary. The article examines the legal nature of digital identification in economic relations. The author considers digital identification as a complex legal institution, analyzes its conceptual definitions, functional aspects, and structural elements. The paper reveals the relationship between the concepts of digital identification, digital identity, digital footprint, and digital profile, and also explores the role of digital identification in ensuring the digital sovereignty of the state. Special attention is paid to the legal status of subjects of digital identification and the significance of this institution for civil law regulation in the digital environment.

Keywords: digital identification, digital identity, digital footprint, digital profile, legal regulation, economic relations, digital sovereignty, digital economy, personal data, information security.

Газизуллин Ришат Ильнурович
доктор юридических наук,
кандидат экономических наук,
Казанский (Приволжский) федеральный университет
Rishat.Gazizullin@kpfu.ru

Аннотация. В статье исследуется правовая природа цифровой идентификации в экономических отношениях. Автор рассматривает цифровую идентификацию как комплексный правовой институт, анализирует ее концептуальные определения, функциональные аспекты и структурные элементы. В работе раскрывается взаимосвязь понятий цифровой идентификации, цифровой личности, цифрового следа и цифрового профиля, а также исследуется роль цифровой идентификации в обеспечении цифрового суверенитета государства. Особое внимание уделяется правовому статусу субъектов цифровой идентификации и значению данного института для гражданско-правового регулирования в цифровой среде.

Ключевые слова: цифровая идентификация, цифровая личность, цифровой след, цифровой профиль, правовое регулирование, экономические отношения, цифровой суверенитет, цифровая экономика, персональные данные, информационная безопасность.

Введение

В условиях стремительной цифровизации всех сфер общественной жизни высокую значимость приобретает научное осмысление правовой природы цифровой идентификации в экономических отношениях. Данная проблематика находится на пересечении технологических инноваций, экономических трансформаций и правового регулирования, что обусловливает ее комплексный характер и требует междисциплинарного подхода к исследованию.

Интенсивное развитие информационно-коммуникационных технологий приводит к формированию новых моделей цифровой идентификации, основанных на применении биометрических параметров, технологии распределенного реестра, искусственного интеллекта и иных инновационных решений. Указанные технологические новации, с одной стороны, способствуют оптимизации экономических процессов, с другой — порождают значительные правовые коллизии, требующие своевременного разрешения. Существующий правовой инструментарий зачастую демонстрирует недостаточную эффективность при регулировании отношений, связанных с использованием цифровых идентификаторов, что актуализирует необходимость научного анализа их правовой природы.

Экономический контекст исследуемой проблематики определяется возрастающей ролью цифровой идентификации как базового элемента современных хозяйственных отношений. Цифровые идентификаторы выступают необходимым условием осуществления электронной коммерции, предоставления финансовых услуг, функционирования цифровых платформ и реализации иных форм экономического взаимодействия в цифровой среде. При этом наблюдается тенденция к интеграции данных цифровой идентификации в рыночную систему — они начинают функционировать по законам товарного обращения, что требует разработки адекватных правовых механизмов регулирования их оборота.

Между тем в нормативном регулировании статуса цифровых идентификаторов есть существенные пробелы. Неопределенность юридической силы различных форм электронной идентификации, отсутствие единообразного подхода к регулированию трансграничной цифровой идентификации, несовершенство механизмов защиты прав субъектов персональных данных — все эти факторы свидетельствуют о необходимости специального юридического анализа исследуемой проблематики.

Особую актуальность в процессах цифровой идентификации получают вопросы обеспечения информационной безопасности и защиты персональных данных. Возрастающие риски несанкционированного доступа к идентификационным данным, их неправомерного использования и модификации требуют разработки комплексных правовых механизмов, обеспечивающих баланс между удобством идентификационных процедур и надлежащим уровнем защиты персональных данных субъектов экономических отношений.

Социальное измерение обозначенной проблематики связано с влиянием систем цифровой идентификации на общественные отношения, включая вопросы цифрового неравенства, доступности идентификационных сервисов для различных категорий населения, этические аспекты использования биометрических данных. Правовое регулирование цифровой идентификации должно учитывать социальные последствия внедрения соответствующих технологий и минимизировать возможные негативные эффекты.

Конкуренция различных моделей цифровой идентификации, разработанных государственными и корпоративными субъектами, актуализирует проблематику цифрового суверенитета и определения юрисдикционных границ в цифровой среде. Данные вопросы также требуют научного осмысления.

Институциональная трансформация систем идентификации, выражающаяся в изменении роли традиционных институтов и формировании новых организационно-правовых моделей управления цифровой идентичностью, также обусловливает актуальность исследования. Разработка эффективных механизмов институционального обеспечения процессов цифровой идентификации представляет собой важную научно-практическую задачу.

Таким образом, комплексное исследование правовой природы цифровой идентификации в экономических отношениях имеет существенное теоретическое и практическое значение для формирования сбалансированного правового регулирования, способствующего защите прав субъектов экономических отношений и устойчивому развитию цифровой экономики. На это обстоятельство неоднократно указывали различные авторы, имея в виду приоритет разработки правовых, экономических, технологических и социально-философских основ формирования эффективной системы идентификации, обеспечивающей доверие участников экономических отношений в цифровой среде[1].

В рамках настоящей статьи предлагаем два рабочих определения цифровой идентификации в ее правовом аспекте:

1) цифровая идентификация — это комплекс правовых норм, технических средств и организационных мероприятий, направленных на однозначное установление связи между физическим или юридическим лицом и его цифровым представлением в информационных системах для целей правоотношений;
2) цифровая идентификация — это правовой институт, регулирующий отношения по установлению и подтверждению цифровой личности субъектов права, обеспечивающий правовую определенность, безопасность и доверие при совершении юридически значимых действий в цифровой среде.

Первое определение концептуализирует цифровую идентификацию через системный подход, интегрирующий три взаимосвязанных компонента: нормативно-правовой, технологический и организационно-процедурный. Нормативно-правовой компонент подразумевает наличие юридически закрепленных правил, регламентирующих процессы идентификации в цифровой среде, что обеспечивает легитимность и правовую определенность данных процессов. Технологический компонент указывает на необходимость использования специальных программно-аппаратных решений, обеспечивающих техническую реализацию идентификационных процедур, их надежность и безопасность. Организационно-процедурный компонент отражает потребность в структурированных алгоритмах действий, протоколах и регламентах, обеспечивающих практическую имплементацию идентификационных механизмов.

[1] Демьянец, М.В. Правовое регулирование идентификации в условиях развития информационно-коммуникационных технологий / М.В. Демьянец // Образование и право. — 2018. — № 1. — С. 104–114; Дудко, М.О. Цифровая идентичность личности: теоретико-правовой аспект // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серия 4. Правазнаўства. — 2019. — Т. 9, № 3. — С. 6–12; Кондаков, А.М., Костылева, А.А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы// Вестник РУДН. Серия: Информатизация образования. — 2019. — Т. 16, № 3. — С. 207–218. — DOI: 10.22363/2312-8631-2019-16-3-207-218; Наумов, В.Б. Институт идентификации в информационном праве: автореферат дисс. … доктора юрид. наук. ИГП РАН. Москва, 2020. 42 с.; Соловьева, Л.Н. Цифровая идентичность как феномен информационной современности// Вестник Военной академии Ракетных войск стратегического назначения. — 2023. — С. 1–12. — URL: https://orcid.org/0000-0001-7490-7084; Степанова, М.Н. Регулирование правоотношений в эпоху цифровой трансформации // Правопорядок: история, теория, практика. 2025. № 1 (44). С. 44–49. DOI: 10.47475/2311-696X-2025-44-1-44-49; Химченко, А.И. Вопросы реализации доверия в условиях развития цифровой экономики // Право и цифровая экономика. 2024. № 1. Доступ из СПС «КонсультантПлюс»; Чернавин, Ю.А. Цифровая идентичность личности: сущность, особенности возникновения и проявления // Человеческий капитал. — 2022. — № 12(168). — С. 74–78.

Определение акцентирует внимание на целевой направленности цифровой идентификации — однозначном установлении связи между реальным субъектом права и его цифровым представлением, что свидетельствует о приоритете верификационной функции данного феномена. Существенным признаком является также указание на двойственность субъектного состава — физические и юридические лица, что расширяет сферу применения данного определения на все категории участников правоотношений.

Детерминация цифрового представления через его локализацию в информационных системах подчеркивает технологическую обусловленность рассматриваемого феномена и его неразрывную связь с цифровой инфраструктурой.

Финальный элемент определения — указание на предназначение «для целей правоотношений» — устанавливает функциональные границы применения цифровой идентификации, локализуя ее в юридически значимом контексте и отграничивая от иных форм установления цифровой личности, не имеющих правового значения.

Ключевым концептуальным элементом второй дефиниции выступает квалификация цифровой идентификации как правового института, что предполагает наличие совокупности юридических норм, объединенных предметным единством и регулирующих определенную группу общественных отношений. Такой подход акцентирует внимание на системности и структурированности правового регулирования, отражая интеграцию цифровой идентификации в общую конструкцию правовой системы.

Определение фиксирует предметную область регулирования — отношения по установлению и подтверждению цифровой личности, что демонстрирует двойственный характер идентификационных процедур: первичное установление цифровой личности и последующее подтверждение ее аутентичности. Использование термина «цифровая личность» позволяет подчеркнуть формирование специфического правового статуса субъекта в цифровом пространстве, отличного от его статуса в физическом мире, но юридически с ним связанного. Дефиниция указывает на субъектный состав регулируемых отношений — «субъекты права», что охватывает весь спектр потенциальных участников правоотношений, включая физических и юридических лиц, а также иных субъектов, признаваемых правом.

Функциональная направленность института цифровой идентификации раскрывается через триаду обеспечиваемых им ценностей: правовую определенность, безопасность и доверие. Правовая определенность предполагает ясность, недвусмысленность и предсказуемость правового регулирования и его последствий. Безопасность указывает на защищенность субъектов от неправомерного доступа к их цифровой личности и связанным с ней данным. Доверие отражает социально-психологический аспект, необходимый для эффективного функционирования цифровых взаимодействий.

Кроме того, определение локализует сферу применения института — «при совершении юридически значимых действий в цифровой среде», что устанавливает функциональные границы регулирования и подчеркивает юридическую значимость как квалифицирующий признак регулируемых действий. Указание на цифровую среду как пространство реализации данного института отражает его технологическую обусловленность и специфику применения в контексте информационно-коммуникационных технологий.

Таким образом, эти определения соотносятся друг с другом как абстрактная модель (1) и ее конкретизация (2). Если в первом определении задана абстрактная концептуальная рамка, охватывающая все потенциальные аспекты цифровой идентификации и намечающая общие контуры феномена, то второе определение фокусируется только на институциональном воплощении цифровой идентификации в правовой системе. В данном случае широкое понятийное поле детализируется на уровне целостного правового института с четко обозначенными функциями (обеспечение правовой определенности, безопасности и доверия) и сферой применения (юридически значимые действия в цифровой среде).

Такое соотношение между определениями можно рассматривать как движение от общего к частному, от абстрактной концептуализации к конкретному правовому механизму. Первое определение создает концептуальный фундамент, а второе — выстраивает на этом фундаменте конкретную правовую конструкцию, адаптированную к потребностям регулирования цифровых правоотношений.

В практическом аспекте под понятийное содержание второго определения подпадают основные виды цифровой идентификации, имеющие целый ряд общих элементов:

1. Биометрическая идентификация, основанная на уникальных физиологических или поведенческих характеристиках субъекта права. Этот вид полностью соответствует концепции правового института, поскольку требует нормативного регулирования процедур сбора, хранения и обработки биометрических данных, а также обеспечивает высокий уровень правовой определенности и безопасности при совершении юридически значимых действий. К данному виду относятся:

— идентификация по отпечаткам пальцев;
— распознавание лица;
— сканирование сетчатки или радужной оболочки глаза;
— голосовая биометрия;
— идентификация по рисунку вен.

2. Электронная цифровая подпись (ЭЦП) и усиленная квалифицированная электронная подпись как правовой механизм подтверждения цифровой личности при совершении юридически значимых действий. Данный вид идентификации непосредственно интегрирован в правовую систему, имеет детальное нормативное регулирование и направлен на обеспечение доверия в цифровой среде.
3. Многофакторная аутентификация, комбинирующая различные методы подтверждения цифровой личности для повышения уровня безопасности. Этот вид соответствует требованию обеспечения безопасности и доверия, заложенному во втором определении цифровой идентификации, и требует правового регулирования процедур комбинирования различных факторов.
4. Идентификация через государственные цифровые платформы и системы, а именно:

— Единая система идентификации и аутентификации (ЕСИА);
— национальные цифровые ID-карты и электронные паспорта;
— системы цифровой идентификации для доступа к государственным услугам.

5. Банковская (финансовая) идентификация, включая удаленную идентификацию клиентов финансовых организаций; системы идентификации для противодействия отмыванию доходов, биометрические системы идентификации клиентов банков.
6. Корпоративные системы цифровой идентификации, используемые юридическими лицами для подтверждения полномочий сотрудников и контрагентов при совершении юридически значимых действий.
7. Системы цифровой идентификации на основе распределенных реестров (блокчейн), обеспечивающие децентрализованное подтверждение цифровой личности при сохранении высокого уровня доверия и безопасности.

Все перечисленные виды цифровой идентификации удовлетворяют признакам, сформулированным во втором определении, поскольку:

— требуют системного правового регулирования (правовой институт);
— направлены на установление и подтверждение цифровой личности субъектов права;
— обеспечивают правовую определенность, безопасность и доверие;
— применяются при совершении юридически значимых действий в цифровой среде.

При этом каждый из видов имеет свою специфику правового регулирования, обусловленную техническими особенностями и сферой применения, что подтверждает институциональный характер цифровой идентификации как комплексного правового явления.

Далее покажем концептуальную иерархию и функциональное соотношение понятий цифровой идентификации, цифровой личности, цифрового следа и цифрового профиля, в которых отражены различные аспекты цифрового существования субъекта в информационном пространстве.

«Цифровой след» представляет собой наиболее фундаментальное и широкое понятие из рассматриваемой группы. Он охватывает совокупность всех данных, которые субъект оставляет в цифровой среде в результате своей активности. Цифровой след формируется как осознанно (активный след), так и неосознанно (пассивный след), включая историю посещений веб-сайтов, поисковые запросы, геолокационные данные, метаданные создаваемых файлов, информацию о подключениях к сетям и многое другое. Принципиально важно, что цифровой след образуется независимо от наличия процедур идентификации и не всегда может быть однозначно связан с конкретным субъектом. Он существует объективно как информационный отпечаток активности в цифровой среде и является своего рода сырьем, из которого при определенных условиях может формироваться цифровая личность.

«Цифровая личность» — более структурированный и целенаправленно формируемый концепт: это совокупность цифровых данных и атрибутов, которые идентифицируют конкретного субъекта в информационном пространстве. В отличие от цифрового следа, цифровая личность предполагает наличие устойчивой связи между информационными элементами и реальным субъектом. Она может включать как официальные идентификаторы (имя пользователя, номер паспорта, ИНН, СНИЛС в их цифровом представлении), так и неофициальные атрибуты (аватары, псевдонимы, репутационные показатели на различных платформах). Цифровая личность обладает определенной целостностью и преемственностью, что позволяет субъекту выступать в качестве стабильного участника цифровых взаимодействий. Важно отметить, что один физический субъект может иметь несколько цифровых личностей в различных системах или для различных целей, а формирование цифровой личности может происходить как по инициативе самого субъекта, так и третьих лиц (например, государства или корпораций).

«Цифровой профиль» можно рассматривать как структурированную, формализованную и институционализированную форму цифровой личности. Это си-

стематизированный набор верифицированных данных о субъекте, организованный в соответствии с определенными стандартами и хранящийся в специализированных информационных системах. Цифровой профиль обычно создается и поддерживается в рамках конкретной платформы, сервиса или государственной системы и содержит данные, необходимые для реализации функционала этой системы. Ключевыми характеристиками цифрового профиля являются его структурированность (данные организованы по определенным категориям), верифицируемость (данные проходят процедуру проверки) и целевое назначение (профиль создается для конкретных задач). В отличие от более аморфной цифровой личности, цифровой профиль имеет четкие границы и состав данных, определяемые требованиями соответствующей информационной системы. Примерами могут служить Единый цифровой профиль гражданина в государственных информационных системах, клиентский профиль в банке или профиль пользователя в социальной сети.

«Цифровая идентификация» выступает как процессуальное понятие по отношению к обозначенным субстантивным концептам. Это динамический процесс установления и подтверждения связи между реальным субъектом и его цифровым представлением (цифровой личностью или цифровым профилем). Как уже было отмечено выше, цифровая идентификация включает комплекс технических, организационных и правовых механизмов, обеспечивающих достоверное соотнесение цифровых данных с конкретным субъектом. Она опирается на цифровой профиль как на структурированный набор верифицированных данных и использует элементы цифрового следа для дополнительной верификации. В процессе цифровой идентификации происходит проверка соответствия предъявляемых субъектом идентификаторов (паролей, биометрических данных, электронных подписей и других) тем данным, которые хранятся в его цифровом профиле, что позволяет установить аутентичность цифровой личности.

Таким образом, выстраивается следующая функциональная взаимосвязь рассматриваемых понятий:

— цифровой след формируется в результате любой активности субъекта в цифровой среде и существует объективно, независимо от процедур идентификации;
— на основе элементов цифрового следа и других данных формируется цифровая личность как комплексное представление субъекта в информационном пространстве;
— цифровой профиль представляет собой структурированную и верифицированную форму цифровой личности, созданную в рамках конкретной информационной системы;
— цифровая идентификация выступает как процесс установления и подтверждения связи между реальным субъектом и его цифровым представлением, опираясь на данные цифрового профиля и элементы цифрового следа.

В контексте правового регулирования цифровой экономики, и особенно ее платформенного сегмента, понимание этих взаимосвязей необходимо для разработки эффективных механизмов защиты прав субъектов, обеспечения безопасности цифровых транзакций и формирования доверительной среды для цифровых взаимодействий.

В качестве иллюстративной аналогии представьте цифровое пространство как огромный город с множеством районов, зданий и улиц.

Цифровой след — это все следы, которые вы оставляете, перемещаясь по городу. Это отпечатки обуви на свежем снегу, случайно оброненные чеки из магазинов, записи камер видеонаблюдения, фиксирующие ваше прохождение, тепловые следы от прикосновений к предметам. Вы создаете эти следы непрерывно и часто неосознанно; они разбросаны по всему городу, и хотя каждый след сам по себе может мало что сказать о вас, собранные вместе они формируют карту вашей активности; при том эти следы существуют независимо от того, представились ли вы кому-то в городе или нет.

Цифровая личность — ваш образ в глазах жителей города. Это совокупность всего, что о вас знают или думают другие: ваша внешность, манера речи, репутация в различных кругах. У вас может быть разная «личность» в разных контекстах: вы можете быть известны как строгий профессор в университете, весельчак в кругу друзей и заботливый родитель в семье. Цифровая личность формируется частично из ваших собственных действий и самопрезентации, частично из того, как вас воспринимают другие, и частично из следов, которые вы оставляете.

Цифровой профиль — это ваше официальное досье в различных учреждениях города. Это структурированная информация о вас в городской администрации, банке, поликлинике, библиотеке, фитнес-клубе. В каждом таком профиле содержатся только те данные, которые нужны конкретному учреждению: в банке — ваша кредитная история, в поликлинике — медицинская карта, в библиотеке — список взятых книг. Эти профили созданы целенаправленно, содержат проверенную информацию и используются для конкретных целей. В отличие от размытой цифровой личности, цифровой профиль имеет четкую структуру и границы.

Цифровая идентификация — это процесс, когда охранник у входа в здание проверяет, действительно ли вы тот, за кого себя выдаете. Он может попросить ваш паспорт (официальный документ), сверить фотографию

с вашим лицом (биометрия), позвонить человеку, который может подтвердить вашу личность (доверенная третья сторона), или задать контрольные вопросы, ответы на которые должны совпасть с информацией в вашем профиле. Цифровая идентификация — это мост между физическим вами и вашим представлением в городских системах.

Теперь представьте, что вы хотите войти в здание банка, чтобы получить кредит. Охранник на входе проверяет ваш паспорт и сканирует отпечаток пальца (цифровая идентификация). После подтверждения вашей личности сотрудник банка обращается к вашему банковскому досье (цифровой профиль), где хранится информация о ваших счетах и кредитной истории. Для принятия решения о выдаче кредита банк может также учесть вашу репутацию в городе и отзывы других учреждений (цифровая личность). В процессе рассмотрения заявки банк может проанализировать данные о ваших перемещениях по городу и покупках (цифровой след), чтобы оценить ваши финансовые привычки и платежеспособность.

Таким образом, цифровой след — это все информационные отпечатки вашего существования в городе, цифровая личность — ваш общественный образ, цифровой профиль — ваше формализованное досье в конкретных учреждениях, а цифровая идентификация — процесс подтверждения, что вы действительно являетесь собой при взаимодействии с городскими системами.

Аналогия с городским пространством помогает также понять истоки распространенных предубеждений относительно цифрового существования субъекта в информационном пространстве. Так, многие проявляют технофобию, то есть опасаются цифровых технологий вообще и биометрии в частности, ссылаясь на страх перед тотальным наблюдением и использованием данных для целей, отличных от изначально заявленных, а также на ощущение беспомощности перед «непонятными» технологическими новшествами. Не менее устойчивыми являются неадекватные представления о том, что цифровой суверенитет неизбежно ведет к изоляции и «цифровому концлагерю».

Между тем в современном государстве, а также в мировых масштабах именно взаимосвязь цифровой идентификации и цифрового суверенитета определяет развитие цифровой экономики, которая трансформирует традиционные отрасли, создает новые рынки и меняет структуру экономических отношений, делая их более горизонтальными, прозрачными и динамичными, где ценность формируется через взаимодействие различных групп пользователей и эффективное использование данных.

В юрисдикционном контексте системы цифровой идентификации устанавливают границы цифрового суверенитета государства посредством определения юрисдикционной принадлежности субъектов в цифровом пространстве. Национальная система цифровой идентификации обеспечивает распространение государственной юрисдикции на идентифицированных субъектов, определение их правового статуса и установление пределов применения национального права. Отсутствие собственной суверенной системы идентификации неизбежно приводит к размыванию юрисдикционных границ и фактической передаче элементов суверенитета внешним акторам.

Технологическая независимость систем цифровой идентификации представляет собой критически важный компонент цифрового суверенитета, включающий контроль над инфраструктурой хранения и обработки идентификационных данных, независимость криптографических алгоритмов и протоколов, собственные технологии биометрической верификации, а также национальные стандарты обмена идентификационной информацией. Использование иностранных технологических решений для критически важных компонентов системы цифровой идентификации создает технологическую зависимость и уязвимость цифрового суверенитета государства.

В информационно-аналитическом аспекте системы цифровой идентификации генерируют значительные массивы данных, анализ которых позволяет формировать стратегически важные сведения о социально-экономических процессах. Суверенный контроль над этими данными обеспечивает независимость в принятии государственных решений, защиту от внешнего информационно-аналитического влияния и возможность проактивного государственного управления на основе предиктивной аналитики. Утрата контроля над данными цифровой идентификации ограничивает аналитический суверенитет государства и создает информационную асимметрию в пользу внешних акторов.

Экономический аспект взаимосвязи проявляется в том, что системы цифровой идентификации становятся фундаментальной инфраструктурой цифровой экономики, определяя возможности экономического суверенитета через контроль над транзакционной инфраструктурой и платежными системами, реализацию национальной экономической политики через идентификационные механизмы, защиту национальных экономических интересов при трансграничном движении данных и формирование условий для развития национальных цифровых платформ и сервисов.

Правовое регулирование цифровой идентификации отражает нормативное измерение цифрового суверенитета, включая законодательное закрепление

национальных стандартов и процедур идентификации, определение правового статуса цифровой личности, установление режима трансграничной передачи идентификационных данных и регулирование вопросов признания иностранных систем идентификации. Отсутствие суверенного правового регулирования приводит к фактическому применению иностранных правовых норм на национальной территории.

Социокультурный аспект взаимосвязи проявляется в том, что системы цифровой идентификации воплощают культурные и ценностные особенности общества, отражая национальные этические нормы в принципах функционирования, учитывая культурные особенности при определении допустимых методов идентификации, соответствуя общественному консенсусу о балансе безопасности и приватности, а также сохраняя культурную идентичность в цифровом пространстве.

Геополитический аспект связи цифровой идентификации и цифрового суверенитета заключается в том, что контроль над системами идентификации становится элементом геополитического влияния и определяет позицию государства в глобальной цифровой экосистеме. Это включает возможность участия в формировании международных стандартов, способность защищать идентификационные данные граждан от иностранного доступа, независимость от геополитически мотивированных ограничений доступа к технологиям и формирование региональных альянсов по вопросам цифровой идентификации.

В контексте национальной безопасности системы цифровой идентификации являются критической инфраструктурой в цифровую эпоху, обеспечивая защиту от цифровых угроз, предотвращение несанкционированного доступа к критическим ресурсам, противодействие цифровой преступности и обеспечение непрерывности функционирования государственных систем в кризисных ситуациях. Зависимость от внешних систем идентификации создает критические уязвимости в системе национальной безопасности.

В аспекте цифровых прав и свобод баланс между государственным контролем и цифровыми правами граждан в системах идентификации определяет модель цифрового суверенитета, включая формирование национальной модели защиты персональных данных, определение границ государственного доступа к идентификационной информации, обеспечение права на «цифровое забвение» и защиту от дискриминации на основе цифрового профиля. Таким образом, цифровая идентификация становится фундаментальным элементом цифрового суверенитета, определяющим способность государства сохранять независимость, защищать национальные интересы и реализовывать стратегические приоритеты в цифровую эпоху[2].

Итак, цифровая идентификация — это сложная многоуровневая система правоотношений, которая характеризуется разнообразием субъектного состава и спецификой соответствующих правовых статусов. Анализ данной сферы позволяет выделить четыре основные категории субъектов: физические лица, юридические лица, государственные органы и операторы систем цифровой идентификации.

Правовое положение физических лиц в системе цифровой идентификации отличается дуализмом, поскольку они одновременно выступают и как субъекты, и как источники идентификационных данных. Их правосубъектность в цифровом пространстве включает право на цифровую идентичность, доступ к системам идентификации, защиту своих данных, информационное самоопределение и «цифровое забвение». При этом на физических лиц возлагаются обязанности по обеспечению достоверности предоставляемых данных, соблюдению правил безопасности, своевременной актуализации информации и уведомлению о компрометации идентификационных данных. Особого внимания заслуживает специфика правового статуса отдельных категорий физических лиц, таких как несовершеннолетние, недееспособные лица, иностранные граждане и публичные фигуры.

Юридические лица в системе цифровой идентификации функционируют в трех основных качествах: как субъекты идентификации, пользователи идентификационных данных и участники инфраструктуры идентификации. В качестве субъектов идентификации они используют цифровые сертификаты, электронные подписи и корпоративные механизмы управления цифровой идентичностью. Как пользователи данных они обязаны обеспечивать безопасность и конфиденциальность полученной информации, соблюдать правовой режим использования идентификационных данных в коммерческих целях. В роли участников инфраструктуры идентификации выступают частные провайдеры услуг, удостоверяющие центры, организации, разрабатывающие технологии и обеспечивающие техническую инфраструктуру.

Государственные органы в системе цифровой идентификации выступают одновременно как регуляторы,

[2] Цифровая диктатура vs цифровой суверенитет: проблемы, риски, возможности. Форум СПБ, 24 апреля 2025, https://forumspb.com/news/news/tsifrovaja-diktatura-vs-tsifrovoj-suverenitet-problemy-riski-vozmozhnosti-/; Бухарин, В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО. 2016. №6 (51). URL: https://cyberleninka.ru/article/n/komponenty-tsifrovogo-suvereniteta-rossiyskoy-federatsii-kak-tehnicheskaya-osnova-informatsionnoy-bezopasnosti (дата обращения: 26.07.2025).

операторы и пользователи систем идентификации. В качестве регуляторов они осуществляют нормативно-правовое регулирование, лицензирование и аккредитацию участников инфраструктуры, надзор и контроль за функционированием систем. Как операторы они создают и эксплуатируют государственные системы идентификации, обеспечивают их интероперабельность, доступность и надежность. В роли пользователей идентификационных данных государственные органы действуют на основании специальных правовых оснований, с соблюдением установленных ограничений и процедур.

Особую категорию субъектов правоотношений в сфере цифровой идентификации представляют операторы соответствующих систем, обеспечивающие функционирование инфраструктуры идентификации и выполняющие ключевые функции по обработке идентификационных данных. Их правовой статус характеризуется наличием специальных требований, включая лицензирование, аккредитацию и сертификацию. Функционал операторов охватывает сбор и верификацию данных, их хранение и актуализацию, обеспечение доступа уполномоченных субъектов, безопасности и конфиденциальности информации.

В российской экономике сформировалась сложная экосистема субъектов правоотношений в сфере цифровой идентификации, где взаимодействуют государственные и частные структуры. Физические лица взаимодействуют с системами цифровой идентификации через ЕСИА, ЕБС и систему электронной подписи. Юридические лица представлены банками, операторами связи, удостоверяющими центрами, маркетплейсами. Ключевыми государственными органами выступают Минцифры, Роскомнадзор, ФНС, Банк России и ФСБ. Среди операторов систем цифровой идентификации выделяются Ростелеком, НСПК, Гознак и аккредитованные удостоверяющие центры. Защита персональных данных при цифровой идентификации сопряжена с комплексом проблем технологического, организационно-правового, социально-этического характера, а также вопросами согласия субъектов, системными проблемами и трудностями международного взаимодействия. Эффективное функционирование системы правоотношений в сфере цифровой идентификации требует баланса интересов всех категорий субъектов, четкого разграничения их прав и обязанностей, а также установления адекватных механизмов ответственности за нарушения в данной сфере.

Цифровая идентификация представляет собой фундаментальный элемент современного гражданско-правового регулирования, значение которого выходит далеко за рамки публичных отношений контроля и надзора.

В контексте гражданского права данный феномен обеспечивает достоверную связь между субъектом права и его волеизъявлением в цифровой среде, что критически важно для действительности электронных сделок. Без надежной цифровой идентификации невозможно гарантировать, что электронную сделку заключило именно уполномоченное лицо, а не третье лицо, неправомерно использующее чужие данные.

Принцип автономии воли, лежащий в основе гражданского права, в цифровом пространстве реализуется именно через механизмы, позволяющие достоверно установить, что волеизъявление исходит от конкретного субъекта, обладающего соответствующими правами. Цифровая личность становится юридически значимым воплощением субъекта в виртуальном пространстве, через которое он осуществляет свою правосубъектность.

С появлением в Гражданском кодексе РФ понятия цифровых прав как особого вида имущественных прав возникла необходимость четкого определения их принадлежности конкретным субъектам, что обеспечивается именно механизмами цифровой идентификации. Цифровой профиль фактически становится вместилищем цифровых прав субъекта. Оборотоспособность современных цифровых активов, включая токены, криптовалюты и NFT, напрямую зависит от надежных механизмов идентификации владельцев и подтверждения перехода прав.

Отметим и то, что развитие договорного права в цифровой среде, включая смарт-контракты и иные формы автоматизированного исполнения обязательств, требует однозначной идентификации сторон и определения носителей прав и обязанностей. В платформенной экономике защита прав потребителей невозможна без надежных механизмов идентификации всех участников правоотношений. Трансформация традиционных механизмов представительства с появлением цифровых агентов и виртуальных ассистентов также основывается на концепциях цифровой идентификации. Наследственное право сталкивается с вызовом определения судьбы цифровых активов после смерти субъекта, а личные неимущественные права получают новое измерение в цифровой среде, где цифровая личность становится проекцией нематериальных благ. Институт гражданско-правовой ответственности в цифровом пространстве требует четкого определения субъекта ответственности за действия, совершенные через цифровые интерфейсы.

Таким образом, концепции цифровой идентификации, цифровой личности и цифрового профиля формируют не инструменты контроля, а необходимую инфраструктуру для реализации базовых институтов гражданского права в цифровой среде, обеспечивая правовую определенность, защиту прав участников

гражданского оборота и создавая условия для воплощения фундаментальных принципов гражданского права в цифровом пространстве.

Заключение

Изложенное позволяет констатировать, что правовая природа цифровой идентификации в экономических отношениях — это комплексная юридическая характеристика института установления и подтверждения личности субъектов экономической деятельности с использованием цифровых технологий. Данный феномен обладает признаком дуализма, выступая одновременно как инструмент реализации прав субъектов в цифровой среде и как самостоятельный объект нормативного регулирования. Межотраслевой характер цифровой идентификации проявляется на стыке информационного, гражданского, финансового и административного права, что отражает многогранность данного института. В правовой природе цифровой идентификации гармонично сочетаются публично-правовые элементы, проявляющиеся в императивном регулировании вопросов безопасности и защиты персональных данных, и частноправовые элементы, выражающиеся в договорном регулировании отношений между субъектами экономической деятельности.

Функциональные аспекты правовой природы цифровой идентификации раскрываются через легитимационную, трансакционную и превентивно-защитную функции. Легитимационная функция устанавливает связь между цифровым представлением субъекта и его правовым статусом, определяет объем правоспособности в цифровой экономике. Трансакционная функция обеспечивает юридическую достоверность субъектного состава экономических отношений и создает правовые гарантии исполнения обязательств. Превентивно-защитная функция служит правовым инструментом предотвращения неправомерных действий и защиты экономических интересов добросовестных участников рынка.

Структурные элементы правовой природы цифровой идентификации включают субъектный, объектный и процедурный компоненты. Субъектный компонент предполагает дифференцированный подход к различным категориям участников — физическим и юридическим лицам, государственным органам и операторам систем идентификации. Объектный компонент охватывает идентификационные данные, средства и процедуры идентификации, а также результаты идентификации как юридические факты. Процедурный компонент регламентирует первичную идентификацию, аутентификацию, авторизацию и верификацию.

Правовую природу цифровой идентификации определяют принципы пропорциональности, технологической нейтральности и баланса интересов. Принцип пропорциональности предполагает соразмерность применяемых средств идентификации характеру экономических отношений. Принцип технологической нейтральности обеспечивает равное юридическое признание различных технологий идентификации при соблюдении установленных требований. Принцип баланса интересов отражает необходимость согласования интересов безопасности и удобства использования, публичных интересов государства и частных интересов субъектов экономической деятельности.

Понимание правовой природы цифровой идентификации имеет не только теоретическое, но и практическое значение, поскольку позволяет выстраивать эффективные модели правового регулирования, обеспечивающие баланс между безопасностью экономических отношений, защитой прав субъектов и стимулированием инновационного развития цифровой экономики. Правовая природа данного института требует комплексного регулирования, учитывающего технологические, экономические, социальные и этические аспекты цифровой трансформации экономических отношений.

ЛИТЕРАТУРА

1. Бухарин, В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО. — 2016. — №6 (51). — URL: https://cyberleninka.ru/article/n/komponenty-tsifrovogo-suvereniteta-rossiyskoy-federatsii-kak-tehnicheskaya-osnova-informatsionnoy-bezopasnosti (дата обращения: 26.07.2025).
2. Демьянец, М.В. Правовое регулирование идентификации в условиях развития информационно-коммуникационных технологий / М.В. Демьянец // Образование и право. — 2018. — № 1. — С. 104–114.
3. Дудко, М.О. Цифровая идентичность личности: теоретико-правовой аспект // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серия 4. Правазнаўства. — 2019. — Т. 9, № 3. — С. 6–12.
4. Кондаков, А.М., Костылева, А.А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы// Вестник РУДН. Серия: Информатизация образования. — 2019. — Т. 16, № 3. — С. 207–218. — DOI: 10.22363/2312-8631-2019-16-3-207-218.
5. Наумов, В.Б. Институт идентификации в информационном праве: автореферат диссертации на соискание ученой степени доктора юридических наук. Институт государства и права Российской академии наук. — Москва, 2020. — 42 с.
6. Соловьева, Л.Н. Цифровая идентичность как феномен информационной современности// Вестник Военной академии Ракетных войск стратегического назначения. — 2023. — С. 1–12. — URL: https://orcid.org/0000-0001-7490-7084.

7. Степанова, М.Н. Регулирование правоотношений в эпоху цифровой трансформации // Правопорядок: история, теория, практика. 2025. — №1 (44). — С. 44–49. DOI: 10.47475/2311-696X-2025-44-1-44-49.
8. Химченко, А.И. Вопросы реализации доверия в условиях развития цифровой экономики // Право и цифровая экономика. — 2024. — № 1. Доступ из СПС «КонсультантПлюс».
9. Цифровая диктатура vs цифровой суверенитет: проблемы, риски, возможности. Форум СПБ, 24 апреля 2025, https://forumspb.com/news/news/tsifrovaja-diktatura-vs-tsifrovoj-suverenitet-problemy-riski-vozmozhnosti-/ (дата обращения: 26.07.2025).
10. Чернавин, Ю.А. Цифровая идентичность личности: сущность, особенности возникновения и проявления // Человеческий капитал. — 2022. — № 12 (168). — С. 74–78.

Журнал «Современная наука: актуальные проблемы теории и практики»