МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В.ЛОМОНОСОВА
ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Рустамов Павел Анварович

Информационно-правовое обеспечение цифровой экономики

Специальность 5.1.2. Публично-правовые (государственно-правовые) науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор Вайпан Виктор Алексеевич

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ……..……..……..3

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ…….....……..15

1.1. Понятие и принципы информационно-правового обеспечения цифровой экономики...…….…….....……...15

1.2. Объекты информационно-правового обеспечения цифровой экономики…….....……...44

1.3. Субъекты информационно-правового обеспечения цифровой экономики…….....……...91

ГЛАВА 2. ИНФОРМАЦИОННОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ…….....……112

2.1. Российское информационное законодательство в области обеспечения цифровой экономики…….....……..……...112

2.2. Зарубежный опыт информационно-правового обеспечения цифровой экономики……..…….....…….137

ГЛАВА 3. ОСОБЕННОСТИ ИНФОРМАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ В ОТДЕЛЬНЫХ СФЕРАХ ЦИФРОВОЙ ЭКОНОМИКИ…….....…….147

3.1. Информационно-правовое обеспечение в сфере цифровых финансовых активов……..…….…….....……..147

3.2. Информационно-правовое обеспечение отношений по осуществлению сделок в цифровом экономике……..……..…..163

3.3. Правовое обеспечение информационных отношений в инвестиционной сфере……...…….……..…185

3.4. Правовое регулирование использования информации ограниченного доступа в цифровой экономике.....208

ЗАКЛЮЧЕНИЕ…….……...……258

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ……263

ВВЕДЕНИЕ

Актуальность диссертационного исследования. Изменения, произошедшие в последние годы в общественной жизни, политике, экономике, научной сфере привели к значительному росту объемов информации.

Комплексная информатизация и цифровизация обусловила появление новых форм политических, экономических, правовых, социальных отношений, возникновение информационной сферы, связанной с информационным обеспечением различных видов жизнедеятельности. Широкое распространение получили информационно-телекоммуникационные технологии, содержанием которых стало формирование информационного ресурса и его сохранение, передача информации, предоставление различного рода информационных услуг. По данным Института статистических исследований и экономики НИУ ВШЭ рост затрат на развитие цифровой экономики по итогам 2021 года превысил доковидные (валовые внутренние затраты на развитие цифровой экономики составили 4,8 трлн. руб., что на 19,3 % выше, чем в 2020 году), а объем передаваемой информации россиянами по информационно-телекоммуникационной сети «Интернет» удвоился – в 2021 году он составил 105 Эбайт[1]. Особенная актуальность работы обусловлена принятием Национальной программы «Цифровая экономика Российской Федерации»[2], рассчитанной на промежуток 2019-2024 гг., реализацией Стратегией развития информационного общества в Российской Федерации[3], а также Доктрины информационной безопасности Российской Федерации[4].

---

[1] Индикаторы цифровой экономики: 2022: статистический сборник / Г.И. Абдрахманова., С.А. Васильковский, К.О. Вишневский, Л.М. Гохберг и др., И60 Нац. исслед. ун-т «Высшая школа экономики». — М.: НИУ ВШЭ, 2023. 332 с.

[2] Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4418 (утратило силу).

[3] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

[4] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7077.

Стратегия развития информационного общества, утвержденная Указом Президента РФ от 9 мая 2017 года, предполагает бурное развитие цифровой экономики, формирование общества знаний, а также построение электронного государства в соответствии с требованиями информационной безопасности[5].

Такая ситуация значительным образом расширила возможности формирования знаний и навыков, которые обеспечили для граждан, субъектов хозяйствования, общества, государства формирование нематериального капитала. Последний по своей мощности является существенным фактором создания преимуществ на любом рынке или в любых взаимоотношениях.

При таких условиях сформировалась ситуация, когда возник разрыв между количеством информации, характеризующей современное бытие, и способностью ее обработать, эффективно использовать и транслировать.

Возникла также проблема информационной дезориентации, которая значительным образом усложнила принятия объективных решений и возможность формирования адекватного поведения субъектами хозяйствования в условиях, когда информация рассматривается в большей степени не как внутренний ресурс, основа осуществления тех или иных процессов, а как средство для повышения эффективности производственных, коммерческих и иных процессов, что остро ставит проблему необходимости обеспечения информационной безопасности.

Учитывая, что информационные проблемы, стоящие перед обществом в последние годы, стали весьма актуальными, им было посвящено значительное количество исследований в различных сферах жизни общества.

В современном мире мы наблюдаем высокую динамическую изменчивость и активное сближение национальных правовых систем, что обусловлено влиянием региональных и международных практик. Это влечет за собой появление новых проблематик и уникальных сценариев в изучаемой области, что, в свою очередь, требует дальнейшего теоретического осмысления и практического подхода.

---

[5] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

С учетом вышеизложенного, становится очевидной необходимость обновления и углубления теоретических основ и методологических приемов, в рамках которых осуществляется сбор и обработка информации для нужд цифровой экономики. Важным аспектом является также разработка более эффективных способов правового регулирования в сфере обмена информацией с акцентом на направления, связанные с обеспечением информационной безопасности бизнес-структур. Все это делает тему исследования предельно актуальной в текущих условиях.

Объектом диссертационного исследования являются отношения в сфере информационно-правового обеспечения цифровой экономики.

Отношения информационно-правового характера складываются между субъектами хозяйствования, предпринимателями и потребителями, а также между хозяйствующими субъектами и публично-правовыми образованиями (через органы государственной власти и местного самоуправления).

Предметом диссертационного исследования выступает совокупность правовых норм, которые регламентируют информационное обеспечение цифровой экономики.

Цель диссертационного исследования заключается в выявлении теоретических закономерностей информационного-правового обеспечения цифровой экономики с публично-правовых позиций и формулирование на этой основе доктринальных и практических положений, направленных на восполнение пробелов правового регулирования информационного обеспечения цифровой экономики.

Цель исследования обусловила необходимость постановки и решения следующих **научных задач**:

1) выявить проблемы, понятия и основополагающие идеи информационно-правового обеспечения цифровой экономики;

2) описать объекты информационно-правового обеспечения цифровой экономики;

3) сформулировать и описать субъектный состав информационно-правового обеспечения цифровой экономики;

4) дать рекомендации по совершенствованию российского законодательства в области информационного обеспечения цифровой экономики;

5) выявить зарубежный опыт информационно-правового обеспечения цифровой экономики;

6) разрешить проблему информационно-правового обеспечения в сфере цифровых финансовых активов;

7) разрешить проблему информационно-правового обеспечения отношений по осуществлению сделок в цифровой экономике;

8) сформулировать теоретические предложения по решению проблемы правового обеспечения информационных отношений в инвестиционной сфере;

9) сформулировать рекомендации по изменениям в сфере использования информации ограниченного доступа в цифровой экономике.

Методологическая база диссертационного исследования формируется посредством применения методов познания, выявленные наукой и апробированные практикой, используя которые автор решал поставленные задачи.

К общенаучным методам относятся:

– анализ – с целью вычленения элементов изученного материала, интерпретации информации, полученной информации;

– синтез – с целью компиляции, полученных данных и формирования новых элементов;

– системно-структурный метод – в ходе классификации отношений, складывающихся в процессе информационного обеспечения деятельности субъектов хозяйствования;

– формально-логический метод – с целью выявления противоречий действующего законодательства в исследуемой сфере и разработки предложений по его совершенствованию;

В работе также применялись частнонаучные методы:

– формально-юридический метод – при анализе содержания норм, регулирующих отношения относительно информационного обеспечения деятельности субъектов хозяйствования, разработке новых норм (изменений в действующие законодательные акты, регулирующие данную группу правоотношений);

– историко-правовой метод – в ходе исследования развития институтов, регулирующих общественные отношения в исследуемой сфере;

– сравнительно-правовой метод – при изучении формирования и развития института информационного обеспечения деятельности цифровой экономики.

Применение данных методов способствовало рассмотрению особенностей правового регулирования информационного обеспечения цифровой экономики, формированию конкретных предложений и рекомендаций по совершенствованию отдельных правовых норм, регулирующих исследуемую область информационного права.

Теоретическая основа и степень разработанности темы диссертационного исследования. Проблемы информационного-правового обеспечения цифровой экономики недостаточно теоретически исследованы, в то время как имеется острая потребность в доктринальном обосновании совершенствования правового (законодательного) регулирования в данной сфере.

Это связано с тем, что изучение отдельных аспектов темы весьма разрозненно и находит свое отражение в различных отраслях российского права (Е.А. Зверева «Правовое регулирование информационного обеспечения предпринимательской деятельности в РФ»[6] по шифру 12.00.03, Ф.Ю. Мытарев «Правовое регулирование информационного обеспечения малого и среднего предпринимательства»[7] по шифру 12.00.14, А.В. Токолова «Правовое регулирование информационных отношений в сфере цифровых финансовых

[6] Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации: дис. … д-ра юрид. наук: 12.00.03. Моск. гос. юр. академия, Москва, 2007. 422 с.

[7] Мытарев Ф.Ю. Правовое регулирование информационного обеспечения субъектов малого и среднего предпринимательства: автореф. дис. … канд. юрид. наук: 12.00.14. М., 2007. 26 с.

активов»[8] по шифру 12.00.13, Е.Е. Кирсанова «Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике»[9] по шифру 12.00.03). В то же время системное многоаспектное научное исследование проблемы информационного-правового обеспечения цифровой экономики отсутствует.

Основу исследования составили труды ученых, в работах которых затрагиваются вопросы, посвященные общетеоретическим проблемам изучаемой области. Существенный вклад в развитие изучаемого проблематики внесли И.Л. Бачило, В.А. Вайпан, Е.А. Зверева, Н.Н. Ковалева, А.В. Морозов, А.В. Минбалеев, В.Б. Наумов, И.М. Рассолов, В.А. Северин, В.А. Токолов, С.Г. Чубукова и другие. Исследуемые проблемы рассматривались учеными-правоведами, представляющие разные отрасли права. Проблемы, посвященные правовому регулированию информации ограниченного доступа затрагивались Ю.А. Крохиной, И.И. Кучеровым, М.Ю. Костенко, А.В. Торшиным. Частные случаи цифровизации рассматривались А.Н. Варламовой (в сфере развития конкуренции на отраслевых рынках), К.А. Ишековым (в сфере образования), Е.И. Колюшиным (в сфере применения инновационных технологий в избирательском процессе), Н.С. Малютиным (в сфере защиты геномной информации), С.А. Авакьяном и С.Н. Шевердяевым (в сфере конституционно-правового регулирования отношений информационного характера).

Исследование информационного обеспечения в разных областях общественной жизни находили отражение в работах Н.М. Заславской, Ф.Ю. Мытарева, Е.А. Зверевой.

Нормативная база диссертационного исследования. В основу исследования легли следующие нормативные правовые акты: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о

[8] Токолов А.В. Правовое регулирование информационных отношений в сфере цифровых финансовых активов: дис. … канд. юрид. наук: 12.00.13. М., 2022. 215 с.

[9] Кирсанова Е.Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: дис. … канд. юрид. наук: 12.00.03. М., 2021. 234 с.

защите информации»[10], Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации»[11], Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[12], Национальная программа «Цифровая экономика Российской Федерации»[13], а также ряд других нормативных правовых актов.

Научная новизна исследования. Диссертация представляет собой первую комплексную работу, посвященную публично-правовым проблемам информационно-правового обеспечения цифровой экономики, и содержащую доктринальные выводы о решении сущностных правовых проблем информационно-правового обеспечения в отдельных сферах цифровой экономики.

В результате проведенного исследования на защиту выносятся следующие **основные положения**:

1. Под информационно-правовым обеспечением цифровой экономики понимается совокупность правовых норм, регламентирующих сбор, хранение, обработку, передачу, анализ и оценку юридически значимой информации с применением компьютерных технологий и информационных систем, которые влияют на осуществление хозяйствующими субъектами деятельности в цифровой экономике, а также юридические механизмы их применения и соблюдения.

2. Информационно-правовому обеспечению цифровой экономики присущи специальные правовые принципы, степень реализация которых обеспечивает его эффективность. Выявлены и сформулированы следующие

---

[10] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

[11] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

[12] Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

[13] Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4418 (утратило силу).

специальные правовые принципы информационно-правового обеспечения цифровой экономики: (1) координирующего информационно-правового воздействия на экономические и связанные с ними общественные отношения; (2) международной согласованности моделей правовой политики в сфере информационного взаимодействия; (3) обеспечения прозрачности использования алгоритмов и моделей искусственного интеллекта и осведомленности пользователей при взаимодействии с ними; (4) осознанного замедления внедрения технологии искусственного интеллекта в информационно-правовой сфере; (5) всеохватывающего бездокументарного взаимодействия в электронной форме; (6) информационной идентификации; (7) правовой интероперабельности.

3. В информационно-правовом обеспечении цифровой экономики следует выделять принцип информационной идентификации, под которым понимается необходимость установления юридической принадлежности информации, прав на ее обработку соответствующим субъектам цифровой экономики. Данный принцип сочетает в себе факт идентификации субъекта и связанную с ним обязанность третьих лиц по недопущению нарушений прав и законных интересов данного субъекта, возникающих при разглашении принадлежащей ему информации и результатов идентификации, алгоритмов и способов такой идентификации.

4. В сфере информационно-правового обеспечения цифровой экономики необходимо закрепить принцип правовой интероперабельности (способности к информационному взаимодействию), под которым понимается возможность и обязанность органов государственной власти и хозяйствующих субъектов взаимодействовать между собой, осуществляя обмен информацией и знаниями в установленном порядке и в очерченных пределах без каких-либо ограничений доступа и реализации. Принцип правовой интероперабельности лежит в основе концепции цифрового управления, реализуемой в рамках построения государственной политики в сфере цифровой экономики, а также необходим для построения единого цифрового рынка.

5. Под субъектами информационно-правовых отношений в широком смысле следует понимать конкретных участников определенных информационно-правовых отношений, основанных на обмене, использовании и распространении информации. Они могут быть классифицированы на: (1) индивидуальных субъектов (физических лиц), участвующих в информационном обмене и обороте; (2) коллективных субъектов (юридических лиц), участвующих в процессах создания, изменения, передачи, распространения, приема и использования информации; (3) органы государственной власти и местного самоуправления, регулирующие информационные процессы и обеспечивающие правоприменение в информационной сфере; а также (4) квазисубъектов, участвующих в информационных процессах (роботы с искусственным интеллектом, нейросети, электронное лицо, цифровая личность и тому подобное).

6. В публично-правовом значении объект, функционирующий на основе технологии искусственного интеллекта, следует рассматривать в качестве источника повышенной опасности, не поддающегося полному контролю человека, использование которого влечет угрозу причинения вреда неограниченному числу лиц. Для защиты публичных интересов и в целях безопасности в сфере информационно-правового обеспечения цифровой экономики использование технологий искусственного интеллекта должно сопровождаться применением обязательного страхования гражданской ответственности владельца (оператора) данного объекта. Применение данной правовой конструкции при использовании технологии искусственного интеллекта обеспечивает ограничение ответственности ее владельцев (операторов) и разработчиков в случаях, когда невозможно однозначно установить их виновность, то есть когда вред причинен из-за допустимого несовершенства технологии искусственного интеллекта (ПО) или ее неконтролируемого действия или бездействия.

7. Инфраструктура цифрового профиля, основанная на единой системе идентификации и аутентификации (ЕСИА), должна содержать публичный реестр согласий субъектов о возможной передаче данных из цифрового профиля третьим лицам, в котором должны содержаться, в том числе, цели такой передачи.

8. В целях обоснованного использования субъектами хозяйствования цифрового профилирования граждан в виде сбора характеристик применяемых компьютерных программ и сведений о лицах, предлагается правовая регламентация механизма уведомления заинтересованных лиц о факте их профилирования и используемых методах. Необходимо закрепить право профилируемых лиц на ознакомление и оспаривание результатов профилирования. Объем предоставляемой для профилирования информации должен быть минимальным, исключающим информацию, которая имеет особое (персональное) значения для субъекта, подвергающегося профилированию. Необходимо установить запрет на выявление в процессе профилирования политических взглядов, религиозной принадлежности и иных внутренних субъективных характеристик лица.

9. В целях эффективного государственного управления инвестиционным процессом и надлежащего информационно-правового обеспечения деятельности по инвестированию средств с использованием инвестиционных платформ необходимо предусмотреть обязанность субъекта, привлекающего финансирование, информировать инвесторов о различных стратегиях вложения средств и их рисках с предоставлением отчетности на всех этапах реализации проекта, а также обязанности заключения соглашения о неразглашении полученной информации до завершения реализации проекта.

10. Правовое регулирование использования данных о цифровых следах и цифровых тенях должно строиться на риск-ориентированном подходе, включающем в себя безопасное, целевое и срочное хранение данных о цифровых следах и цифровых тенях в обезличенной форме (с возможностью деанонимизации информации самим субъектом либо на основании судебного акта).

Теоретическая значимость диссертационного исследования заключается в том, что доктринальные предложения по изменению информационно-правового регулирования цифровой экономики на современном этапе могут быть использованы в науке информационного и цифрового права. Важное теоретическое значение имеют исследования и выводы о категориально-понятийном аппарате в

изучаемой сфере, о правовых механизмах, которые применяются в области информационного обеспечения с участием хозяйствующих субъектов.

Результаты и заключения, полученные в рамках данного исследования, могут найти свое применение в процессе теоретического анализа основ и деталей информационно-правового сопровождения в области цифровой экономики. Также они могут быть востребованы для выявления специфики обеспечения информационной безопасности при проведении подобных исследований.

Практическая ценность работы: работа полезна в практической деятельности юристов – специалистов в сфере информационного и цифрового права, организации деятельности в сфере цифровой экономики, а также результаты исследования могут быть внедрены в учебный процесс. В рамках исследования описывается и обосновывается ряд способов решения практических проблем. Судебная практика и зарубежный опыт, использованные в рамках настоящего исследования, могут лечь в основу обновления учебных программ, а также проведения дальнейших исследований по выбранной тематике.

Практическая ценность диссертационного исследования находит отражение в сформулированных рекомендациях по совершенствованию действующего законодательства.

Личный вклад автора. Выносимые на защиту положения диссертационного исследования получены автором самостоятельно.

Эмпирическая база исследования включает судебную и правоприменительную практику, исследования В.А. Вайпана, Е.А. Зверевой, А.В. Морозова, Ф.Ю. Мытарева, И.М. Рассолова, В.А. Северина, С.Г. Чубуковой и других автором, а также информацию в сети Интернет по вопросам, затрагивающим различные аспекты исследуемой проблематики.

Степень достоверности результатов исследования. Достоверность полученных результатов обеспечивается применением научных методов исследования, подтверждается трудами ученых-правоведов, нормативными правовыми актами, судебными актами.

Апробация результатов исследования. Основные положения и выводы, полученные в ходе диссертационного исследования, изложены в семи научных работах, включая научные статьи, опубликованные в журналах из Перечня Высшей аттестационной комиссии, пять из которых, опубликованы в научных изданиях, рекомендованных для защиты в диссертационном совете МГУ, а также в научных докладах на различных конференциях, в том числе на VI Международной конференции «Информационное общество, цифровая экономика и информационная безопасность» организованной кафедрой компьютерного права и информационной безопасности Высшей школы государственного аудита (факультет) Московского государственного университета имени М.В. Ломоносова, XVI Всероссийской научно-практической конференции с международным участием, посвященной памяти профессора Ф.М. Рудинского и приуроченной к 30-летию МГПУ.

Структура диссертации. Структурно работа состоит из введения, трех глав (первая глава содержит три параграфа, вторая глава включают в себя два параграфа, третья глава – четыре параграфа), заключения.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

§ 1.1. Понятие и принципы информационно-правового обеспечения цифровой экономики

Термин «цифровая экономика» был введен сравнительно недавно – в 1995 году американским ученым из Массачусетского университета Н. Негропонте. Он использовал его для обозначения концепции, объясняющей преимущества новой экономики, которая стала возможной благодаря бурному развитию информационно-коммуникационных технологий, по сравнению с традиционной экономикой[14]. В России понятие цифровой экономики получило дальнейшее развитие в рамках «Стратегии развития информационного общества Российской Федерации на 2017–2030 годы»[15]. Согласно этому документу, цифровая экономика позволяет значительно повысить эффективность различных производственных процессов и сфер деятельности, включая технологии, оборудование, склады, а также процессы продаж и доставки товаров и услуг[16]. В свою очередь, Д. Тапскотт в своей книге «Цифровая экономика: обещания и опасность в эпоху сетевого интеллекта» (1996) предложил свою трактовку понимания цифровой экономики как «экономики, основанной на использовании информационных технологий»[17]. В своей работе Д. Тапскотт подчеркивает, что благодаря внедрению новых технологий появляется новый тип бизнеса, и с того времени ученые и исследовательские институты продолжили уточнять как структуру, так и рамки цифровой экономики[18].

---

[14] Negroponte N. Being Digital. N.Y.: Knopf, 1995. 243 p.

[15] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

[16] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

[17] Tapscott D. The Digital Economy: Promise and Peril In The Age of Networked Intelligence. N.Y.: McGrawHill, 1996. 342 p.

[18] Там же. С. 147-151.

Т. Мезенбург в 2001 году представил концепцию цифровой экономики, выделив три ключевых компонента этой области. Во-первых, он отметил значимость инфраструктуры электронной коммерции, включающей оборудование, программное обеспечение, телекоммуникационные сети и человеческий капитал. Во-вторых, особое внимание было уделена электронная коммерция. Третьим компонентом Т. Мезенбург выделил электронный бизнес – любой бизнес-процесс, организованный через компьютерные сети[19].

Начиная с середины 2000-х годов, когда социальные сети начали активно распространяться, а интернет-инфраструктура развивалась быстрыми темпами, стало очевидно, что выделенные Т. Мезенбургом компоненты цифровой экономики недостаточны для полного охвата всех граней этого явления. Всемирный банк предложил свою трактовку, определив цифровую экономику как выстроенную на применении цифровых информационно-коммуникационных технологии систему отношений в культурной, социальной и экономической сферах. Британский экономист М. Скилтон описывает цифровую экономику как часть новой цифровой экосистемы, представляя ее в виде набора виртуальных активов и цифровых транзакций, осуществляемых на рынках. Также он подчеркивает, что цифровая экономика включает компании, активы и услуги, которые способствуют росту ВВП и улучшению чистого благосостояния. Цифровая экосистема, по его мнению, отражает взаимодействие рыночных технологий и предпринимательской деятельности, что, в свою очередь, приводит к появлению новых типов потребителей, предприятий и рыночных условий, а также изменяет потребительский опыт[20].

Власти Австралии рассматривают цифровую экономику в качестве всемирной основы экономических и социальных процессов, которым

---

[19] Mesenburg T.L. Measuring the Digital Economy / T.L. Meysenbourg. – U.S. Bureau of the Census, 2001. URL: https://www.census.gov/content/dam/Census/library/working-papers/2001/econ/umdigital.pdf (дата обращения: 03.08.2025).

[20] Skitlon M. Building the Digital Economy Enterprice: A Guide to Constructing Monetization Models Using Digital Technologies. Berlin: Springer. 2015. – Access mode: free. URL: https://books.google.ru/books?id=mtRgCgAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата обращения: 03.08.2025).

способствуют такие технологические платформы, как «Интернет», мобильные коммуникации и сенсорные технологии.

В этом контексте цифровая среда рассматривается как основа, на которой строится развитие всех аспектов экономики, а также как ключевой элемент, требующий государственной поддержки для дальнейшего прогресса цифровизации. В свою очередь, правительство Великобритании интерпретирует цифровую экономику как совокупность процессов, связанных с производством цифрового оборудования, распространением средств массовой информации, а также с разработкой программного обеспечения и его программированием[21].

Лидеры стран G 20 определили цифровую экономику как широкий спектр экономической деятельности, включающий использование оцифрованной информации и знаний в качестве ключевого производственного фактора, современные информационные сети как важную сферу деятельности и эффективное использование информационных и коммуникационных технологий как значимый фактор экономического роста и оптимизации структуры экономики. В данном определении акцент сделан на тех видах экономической деятельности, которые непосредственно осуществляются с применением ИКТ и интеллектуальных сетей.

Цифровая экономика является предметом активного изучения в различных научных и исследовательских центрах. Так, Исследовательский центр Economist и компания IBM предлагают свою трактовку, определяя цифровую экономику как такую, которая предоставляет высококачественную инфраструктуру информационно-коммуникационных технологий (ИКТ) и использует возможности этих технологий на благо потребителей, предприятий и органов государственной власти. В свою очередь, аналитики компании Gartner характеризуют цифровую экономику как процесс создания, потребления и управления стоимостью, связанной с цифровыми продуктами, услугами и ресурсами, используемыми организациями. Эксперты из Boston Consulting Group заявляют, что цифровая

[21] Хасаншин И.И. Цифровая экономика: понятие и термины // Московский экономический журнал. 2021. № 4. С. 265-274.

экономика представляет собой процесс применения интернет-связи и передовых цифровых технологий всеми элементами экономической системы, включая как индивидуальных пользователей, так и крупные компании и государственные органы[22].

Из представленных данных, очевидно, что можно выделить два основных подхода к пониманию цифровой экономики. В узком смысле это вид экономической активности в «Интернете», включая такие сферы как электронная коммерция, цифровые финансовые операции и онлайн-услуги. В более широком значении, данное понятие отражает преобразование общества, в целом, благодаря широкому применению информационно-телекоммуникационных технологий, что кардинально изменяет стандарты всех сторон жизни.

Под цифровой экономикой понимается каждый сектор экономики, в котором используются информационно-коммуникационные технологии[23].

Исследовательское издательство The Conversation объясняет, что цифровая экономика отражает то, как цифровые технологии влияют на производство и потребление, «включая то, как товары и услуги продаются на рынке и оплачиваются»[24].

Цифровая экономика охватывает всемирные процессы экономического взаимодействия, торговых сделок и профессионального сотрудничества, интегрируемые и оптимизированные с помощью технологий в области информационных и коммуникационных систем (ИКТ).

Д. Тэпскотт впервые ввел термин «цифровая экономика» в 1996 г. в работе «Цифровая экономика: обещания и опасность в эпоху сетевого интеллекта». Прямого определения в данном исследовании нет, и автор под цифровой экономикой понимает положение, когда речь идет не только о создании сетей технологий, умных машинах, но о взаимодействии людей с помощью технологий, которые сочетают интеллект, знания и креативность для прорывов в создании

---

[22] Там же.

[23] Digital Economy Definition: 3 Digital Economy Examples. URL: https://www.masterclass.com/articles/digital-economy (дата обращения: 02.03.2025).

[24] What Is the Digital Economy? URL: https://online.wharton.upenn.edu/blog/what-is-the-digital-economy/ (дата обращения: 02.03.2025).

богатства и социальном развитии. Подчеркивалось, что цифровая экономика объясняет взаимосвязь между новой экономикой, новым бизнесом и новыми технологиями, а также то, как они дополняют друг друга[25].

Н. Негропонте описал цифровую экономику как использующую «биты вместо атомов»[26].

В заре своего развития термин «цифровая экономика» был синонимичен понятиям, таким как «интернет-экономика», «новая экономика» или «веб-экономика», подчеркивая ее тесную связь с Интернетом.

Тем не менее, данная сфера деятельности обладает более высоким уровнем развития и сложности, по сравнению с простым использованием «Интернета» для экономической выгоды, что Е.Н. Смирнов ассоциирует с основой интернет-экономики[27].

Цифровая экономика знаменует собой эволюционный сдвиг от эпохи третьей промышленной революции к эре четвертой. Третья промышленная революция, часто упоминаемая как цифровая, олицетворяет собою кардинальное преобразование на исходе XX века, когда произошел переход от аналоговых и механических устройств к рождению и широкому применению цифровых технологий.

Четвертая промышленная революция, возникшая на фундаменте предыдущих технологических достижений, усиливает взаимосвязь между физическим пространством и цифровыми, кибернетическими пространствами, беспрестанно расширяя горизонты современных технологий.

Данный процесс представляет собой не просто трансформацию способов экономической деятельности с использованием цифровых сетей, но и ведет к глубокой интеграции цифровых инноваций во все аспекты жизни общества. Это повлекло за собой переосмысление методов управления, производства и

---

[25] Tapscott D. The Digital Economy: Promise and Peril In The Age of Networked Intelligence. N.Y.: McGrawHill, 1996. 342 p.

[26] Об итогах социально-экономического развития Российской Федерации в январе — декабре 2021 г. // Официальный сайт Министерства экономического развития Российской Федерации. URL: http://economy.gov.ru/minec/activity/sections/inforientedsoc (дата обращения: 10.11.2023).

[27] Смирнов Е.Н. Эволюция инновационного развития и предпосылки цифровизации и цифровых трансформаций мировой экономики // Вопросы инновационной экономики. 2018. Т. 8. № 4. С. 553-564.

дистрибуции товаров и услуг, обуславливая необходимость в новых навыках, стратегиях и подходах для эффективного развития и поддержки устойчивых моделей ведения бизнеса в современном мире.

Термины «веб-экономика», «новая экономика» и «интернет-экономика» часто являются взаимозаменяемыми и сводятся к общему понятию «цифровая экономика» — сектор, сфокусированный на применении цифровых и вычислительных инноваций. Такие нововведения в информационные технологии, экономический контекст, в котором они расцветают, а также модели поведения и активности людей, подвергаются радикальным изменениям на фоне глобализации этого нового экономического порядка. Понятие «цифровой экономики» подразумевает охват множества сфер человеческой деятельности, в их числе экономическая, социальная и культурная составляющие.

В каждой из этих областей ключевую роль играют современные информационно-коммуникационные технологии, которые формируют новые подходы к организации процессов, обмену информацией и взаимодействию между субъектами. Влияние цифровых решений прослеживается как в хозяйстве, так и в общественной и социокультурной жизни, где они существенно расширяют возможности развития, взаимодействия и распространения знаний.

Современные трактовки цифровой экономики, в большей мере, обращаются к ее структуре и определяющим элементам. К примеру, выделяют ключевые столпы, которые включают в себя развитие «Интернета», электронную коммерцию между компаниями, цифровую доставку продуктов и услуг, а также традиционную розничную торговлю физическими товарами. Эти компоненты служат фундаментом для того, чтобы кардинально преобразовать традиционные подходы к бизнесу и коммерческой деятельности, открывая путь для инноваций и эффективности и находя отражение в эволюции экономической мысли и практики[28].

На данный момент отчетливо заметен стремительный рост и расцвет

[28] European Commission. Expert Group on Taxation of the Digital Economy. European Commission, Brussels [Электронный ресурс]. URL: http://ec.europa.eu/taxation customs/sites/taxation/files/resources/documents/taxation/gen info /good governance matters/digital/general issues.pdf (дата обращения 10.11.2023).

цифровых платформ, которые все более акцентируют свое влияние на обиходную жизнь людей. Повседневные пользователи таких платформ испытывают определенную степень привязанности к ведущим соцсетям: «Instagram»[29], «Facebook»[30], «Twitter», которые формируют новый вид интерактивных сообществ и влияют на формирование общественного мнения.

Этот феномен цифровизации общества ведет к необратимым изменениям в том, как мы общаемся, проводим бизнес, учимся и развлекаемся. Цифровые товары и услуги предлагают потребителям удобство и доступность, а цифровые технологии, такие как искусственный интеллект, ускоряют инновации, содействуют росту производительности и оптимизации процессов.

Между тем, Интернет вещей (IoT — Internet of Things) соединяет устройства в глобально взаимосвязанную сеть, позволяя производить безостановочный обмен данными между оборудованием и улучшая качество жизни человека через автоматизацию и интеллектуализацию окружающего пространства.

В рамках правового поля определение цифровой экономики содержится в «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Цифровая экономика представляет собой экономическую активность, в основе которой лежат данные в электронном формате. Ключевое преимущество состоит в том, что анализ и обработка больших объемов данных способствуют значительному повышению эффективности в производственных операциях, техниках и методиках управления продажами, а также в логистике товаров и услуг, если сравнивать с предшествующими методами бизнес-практики[31].

Для рассмотрения исследуемой категории полноценно, по мнению автора, представляется интересным исследовать ряд смежных категорий: правового

---

[29] Принадлежит компании Meta, признанной экстремисткой и запрещенной на территории Российской Федерации.

[30] Принадлежит компании Meta, признанной экстремисткой и запрещенной на территории Российской Федерации.

[31] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

обеспечения, информационного обеспечения, а также информационно-правового обеспечения.

Стоит начать с общей категории «правовое обеспечение». В правовой литературе понятие «правовое обеспечение» раскрывается по-разному. Одни ученые рассматривают «правовое обеспечение» как синоним понятия «правового регулирования»[32]. В то время как другие представители юридической науки видят правовое обеспечение как либо комплекс правил (норм), установленных в законодательных актах для нормирования поведения определенных участников, либо как процесс правоприменительной деятельности со стороны этих самых субъектов[33]. Кажется ошибочным отождествление правового обеспечения с процессом правового регулирования, который, в свою очередь, включает в себя набор правил и нормативных актов, разработанных для упорядочивания действий различных правовых субъектов или с самостоятельной правовой практикой. В действительности правовое обеспечение вбирает в себя указанные аспекты и, таким образом, формирует среду, приводящую к реализации уникальной целевой функции обеспечения. Оно является комплексной системой, сочетающей в себе эти элементы для обеспечения порядка и правопорядка в социуме таким образом, чтобы достигались поставленные перед ним цели.

Термин «правовое обеспечение» широко используется в правовой науке, однако, как правило, исследователи прибегают к его применению без попыток дать четкое определение, полагая понятие самоочевидным. Лишь отдельные авторы считают нужным раскрыть содержание этого термина, но часто в контексте специфики своего исследования. Общей чертой всех подходов является связь правового обеспечения с правовым воздействием.

---

[32] Ашихмин И.М. Международно-правовое обеспечение экологической безопасности в военной деятельности : дис. … канд. юрид. наук: 12.00.10. М., 1997. 199 с.

[33] Стахов А.И. Административно-публичное обеспечение безопасности в РФ: автореф. дис. … д-ра юрид. наук: 12.00.14. М., 2007. 35 с.; Редкоус В.М. Административно-правовое обеспечение национальной безопасности в государствах – участниках СНГ: автореф. дис. … д-ра юрид. наук: 12.00.14. М., 2011. 48 с.; Красинский В.В. Правовое обеспечение защиты конституционного строя России в избирательном процессе: автореф. дис. … д-ра юрид. наук: 12.00.02. М., 2011. 48 с.

Ю.А. Тихомиров, анализируя категорию правового обеспечения в рамках управленческой деятельности, характеризует его как комплекс всех форм юридического посредничества, имеющего важные связи с прочими способами обеспечения деятельности организации, к примеру, с информационной поддержкой или обеспечением необходимыми кадрами. Это подчеркивает мульти дисциплинарный характер и значимость правовых процессов в контуре эффективного административного управления.

В состав элементов правового обеспечения правовед включает такие аспекты, как издание правовых актов, их изучение, правовое воспитание, правильное применение правовых норм, анализ правоприменительной практики, контроль за соблюдением законности и совершенствование правовых актов[34]. Таким образом, правовое обеспечение трактуется как снабжение правовыми средствами, что охватывает различные виды юридической деятельности.

В.С. Белых подчеркивал, что правовое обеспечение следует рассматривать как один из видов юридической деятельности. Основной задачей является создание и поддержание необходимого уровня правового регулирования общественных отношений. При этом обеспечение осуществляется через применение как общеобязательных правовых норм, так и ненормативных правовых средств[35]. Е.Б. Лаутс предлагает более узкое толкование термина, рассматривая «правовое обеспечение» как часть процесса правового регулирования, сосредоточенную на достижении его цели в рамках конкретных отношений[36]. В то же время К.И. Амирбеков делает акцент на субъективной стороне права, предлагая трактовку правообеспечительной деятельности как деятельности публично-властных субъектов, выполняемой в рамках установленных процессуально-правовых форм. Основной целью этой деятельности выступает поддержание и устойчивое развитие состояния правообеспеченности. К.И. Амирбеков определяет правообеспеченность как «реальное состояние, характеризующееся постоянным воспроизводством и

---

[34] Тихомиров Ю.А. Курс административного права и процесса. М.: Юринформцентр, 1998. С. 63-66.

[35] Белых В.С. Гражданско-правовое обеспечение качества продукции, работ, услуг : автореф. дис. … д-ра юрид. наук: 12.00.03. Екатеринбург, 1994. С. 4.

[36] Лаутс Е.Б. Правовое обеспечение стабильности рынка банковских услуг : автореф. дис. … канд. юрид. наук: 12.00.03. М., 2007. С. 17.

гарантией верховенства прав человека. Это состояние проявляется в возможности реализации субъективных прав, исполнении правовых обязанностей, соблюдении правовых запретов, поддержании правовых стимулов, а также в сохранении баланса между наделением правами и их ограничением, закрепленными в развитой системе законодательства»[37]. В рамках предложенной концепции правообеспеченность рассматривается наравне с такими категориями, как законность, конституционность и правопорядок, представляя собой высшую форму «правозаконности», «правоконституционности» и «правопорядка»[38]. Таким образом, можно выделить несколько ключевых аспектов, объединяющих разные подходы к определению правового обеспечения. Во-первых, правовое обеспечение представляет собой форму юридической деятельности. Во-вторых, оно носит целенаправленный и правомерный характер, предполагающий строгое соблюдение установленных процедур. В-третьих, правовое обеспечение осуществляется только компетентными институциональными структурами. Среди предложенных трактовок наиболее продуктивным является подход, предложенный В.С. Белых. Его концепция акцентирует внимание на регулирующем воздействии права, которое охватывает не только правовое регулирование, но и процесс реализации (осуществления) правовых норм. При этом информационное и ценностно-ориентационное воздействие права остается за рамками правового обеспечения, что способствует более четкой его идентификации и функциональному разграничению.

Необходимо отметить, что категории информационного обеспечения как самостоятельному элементу не уделялось достаточного внимания. В нормативных правовых актах отсутствует раскрытие информационного обеспечения, ограничиваясь его упоминанием, без детального раскрытия понятия[39].

---

[37] Амирбеков К.И. Правообеспечительная юридическая деятельность: проблемы теории и практики : дис. … д-ра юрид. наук: 12.00.01. Сев.-Кавказ. акад. гос. службы. Ростов н/Д., 2006. 46 с.

[38] Амирбеков К.И. Правообеспечительная юридическая деятельность // Государство и право. 2006. № 1. С. 88-94.

[39] Глава 7 Градостроительного кодекса Российской Федерации от 29.12.2004 № 190-ФЗ (с изм. и доп., вступ. в силу с 01.03.2025) // Российская газета. 30.12.2004. № 290; Раздел 4 Федерального закона «О рынке ценных бумаг» от 22.04.1996 № 39-ФЗ (ред. от 23. 05.2025) // Российская газета. 25.04.1996. № 79.

Законодатель, преимущественно, описывает составные элементы информационного обеспечения.

В доктрине преимущественное количество работ на тему информационного обеспечения связанны с какой-то иной дисциплиной правового характера, вопрос в них раскрывается не полностью либо не затрагивается вовсе[40]. В силу наличия различного подхода к исследованию темы, образуется расхождение в области понятийно-категориального аппарата.

Так, Е.А. Зверева определяет информационное обеспечение как процесс формирования правового механизма, главной задачей которого является удовлетворение информационных потребностей участников предпринимательской деятельности[41].

Е.В. Зайченко под информационным обеспечением в гражданском и арбитражном процессе понимает деятельность судебных органов, а также участников судебного процесса, по поводу предоставления и получения необходимой информации о находящемся в производстве деле[42].

Похожей точки зрения придерживается Г.Н. Кулешов, который под информационным обеспечением в системе государственной гражданской службе подразумевает деятельность уполномоченных субъектов по предоставлению, получению, обработке, размещению информации, а также предоставлению необходимой информации в срок[43].

Изучив ряд авторских определений, можно сделать вывод о том, что подходы к определению информационного обеспечения разнятся в зависимости от исследуемой области. Некоторые ученые определяют понятие как правовой

---

[40] Заславская Н.М. Информационное обеспечение в цифровом обществе (на примере государственного экологического управления) // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И.Р. Бегишева, Е.А. Громовой, М.В. Зазоило, И.А. Филиповой, А.А. Шутовой. В 6 т. Т. 1. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. 560 с.

[41] Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации : дис. … д-ра юрид. наук: 12.00.03. Моск. гос. юр. акад. М., 2007. 422 с.

[42] Зайченко Е.В. Информационное обеспечение в гражданском и арбитражном процессе : дис. … канд. юрид. наук: 12.00.15. Моск. гос. университет. М., 2013. 290 с.

[43] Кулешов Г.Н. Административно-правовое регулирование информационного обеспечения в системе государственной гражданской службы Российской Федерации : дис. … канд. юрид. наук: 12.00.14. Моск. гум. университет. М., 2010. 223 с.

механизм, что отчасти может быть оправданным, но вместе с тем, не отвечает всем нюансам, например, оставляя за рамками информационные системы (как техническую категорию). Право всегда вторично, оно обслуживает сложившиеся отношения, следовательно, информационные системы разрабатываются и применяются субъектами вне зависимости от наличия правового механизма (норм права), за исключением случаев, когда использование информационных систем ограниченно законодательством.

Однако можно возразить, что информационное обеспечение представляет собой деятельность, ориентированную на создание, сохранение и передачу информации. Такой подход видится более соответствующим современным реалиям. Информационное обеспечение рассматривается как сложная категория, включающая в себя несколько самостоятельных компонентов: производство информации, ее предоставление, передачу, распространение, защиту, а также функционирование информационных систем, которые обеспечивают выполнение перечисленных процессов. При наличии всех перечисленных элементов можно говорить о формировании полноценного информационного обеспечения. Можно предположить, что попытка унифицировать категорию информационного обеспечения не представляется возможной, так как данная категория неразрывно связана именно со сферой своего регулирования (и опытом специалистов, которые формулируют категорию).

Информационно-правовое обеспечение, в контексте цифровой экономики, можно рассматривать как совокупность информационных систем (информационных ресурсов) и их правового обеспечения либо исключительно как совокупность норм информационного права, которые регулируют цифровую экономику[44].

Н.А. Троян анализирует информационное-правовое обеспечение через утраченную легальную категорию информационного ресурса. Под информационно-правовым ресурсом следует понимать совокупность документов

[44] Кусова Е.А. Информационно-правовое обеспечение государственного управления // Вестник ТГУ. 2011. № 4. С. 292-295.

правового характера (правовые акты, стратегические программно-целевые документы, акты правоприменительной практики, акты толкования законодательства и так далее), размещенных в цифровом формате на электронных платформах (в том числе, государственных реестрах (регистрах), электронных библиотеках, электронных архивах и так далее)[45].

Следовательно, представляется актуальным сформулировать авторский логический конструкт двух взаимосвязанных определений: информационного обеспечения и информационно-правового обеспечения. *Информационное обеспечение в сфере цифровой экономики представляет собой комплекс организационно-технических средств, направленных на поиск, создание, получение, предоставление, передачу, распространение и защиту информации*. Важной составляющей такого обеспечения выступают информационные ресурсы, способные влиять на функционирование и эффективность деятельности субъектов цифровой экономики.

Под информационно-правовым обеспечением цифровой экономики понимается совокупность правовых норм, регламентирующих сбор, хранение, обработку, передачу, анализ и оценку юридически значимой информации с применением компьютерных технологий и информационных систем, которые влияют на осуществление хозяйствующими субъектами деятельности в цифровой экономике, а также юридические механизмы их применения и соблюдения[46]. Нормы права, которые затрагивают сферу информационного обеспечения, представляют собой совокупность норм как публичного, так и частного права.

Публичная составляющая в исследуемых правоотношениях состоит в наличии следующих категорий: право на информацию, свобода информации, присутствие в отношениях представителей государственной власти (органов местного самоуправления).

---

[45] Троян Н. А. Информационно-правовое обеспечение развития национальной системы правовой информации в Российской Федерации в условиях цифровой трансформации // Мониторинг правоприменения. 2020. № 4 (37). С. 29.

[46] Рустамов П.А. О категории информационно-правового обеспечения цифровой экономики // Евразийская адвокатура. 2025. № 1 (72). С. 157-161.

Частная составляющая заключается в том, что информация может выступать объектом гражданских правоотношений, в силу статьи 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[47].

Осознание информационно-правового обеспечения цифровой экономики разумнее дополнить рассмотрением принципов, так или иначе, влияющих на формирование данной научной категории.

На сегодняшний день в отечественной правовой науке продолжает существовать точка зрения о том, что принципы права в полной мере возможно отождествить с нормами права, что лишь благодаря им правоприменитель способен относиться к принципам права как к непосредственно действующим категориям, явным образом зафиксированным и понятным[48]. Стоит отметить, что наличие двух категорий обуславливает их существование, а именно, отличительной чертой принципа права является то, что он хоть и является нормой права, но представляет собой фундаментальную сущность. Другими словами, можно аргументировать позицию тем, что норма (в фактическом выражении) представляет собой конкретную категорию, не отличающейся фундаментальной устойчивостью, в то время как принцип представляет собой идеологическую категорию, обосновывающую появление нормы, следовательно, он более статичен, фундаментален. В то же время, если рассматривать норму и принцип как логический конструкт, предшествующий облечению их в материальную форму, то можно сказать, что принцип – это следствие, норма – это причина.

Во многих научных статьях ученых – юристов, занимающихся проблемой исследования понятия, классификации, сущности принципов российского права, их роли и места в механизме правового регулирования, высказывается точка зрения

---

[47] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

[48] Алешкова И.А., Власова Т.В. К вопросу о принципах права // Вестник Кыргызско-Российского Славянского университета. 2019. Т. 19. № 7. С. 80.; Панченко В.Ю., Власенко В.Н. Принципы и нормы права как абстрактные и конкретные правовые регуляторы // Российское правосудие. 2020. № 1. С. 15.; Азархин А.В., Карев Д.А., Михайлова М.С. Понятие и классификация правовых принципов // Евразийская адвокатура. 2020. № 1 (44). С. 100.

о необходимости подвергнуть принципы российского права исключительно формальной правовой регламентации[49].

Авторы считают, что закрепление исчерпывающего перечня принципов российского права в текстах основных российских кодексов и законов позволит обеспечить полное единство в их трактовке и реализации со стороны правоприменителей, снизит возможные «ошибки» в правоприменительной деятельности. Остальные же принципы права, не получившие своего легального, письменного выражения в начальных статьях законодательных актов не следует применять вовсе. Излишним трудом явилось бы выведение и формулирование в процессе правоприменительной деятельности принципов права, поскольку это может противоречить воле законодателя, сбивать с толку правоприменителя. Необходимость, адресованная к правоприменителю, руководствоваться собственным правосознанием, опираясь на свою совесть и нравственное воспитание, основы правовой доктрины, оценивать принимаемые решения с позиции справедливости в последнее время стали подвергаться усиленной критике[50]. Выискивание «иллюзорных», «своеобразно понятых» принципов права, по мнению ученых, не способно отразить идеалы справедливости, равенства, гуманизма, понятно и доступно выраженных в текстах большинства законов.

Традиция рассматривать принципы права как особую разновидность обычных норм права, со всеми присущими правовым нормам признаками, по-прежнему сохраняет свое широкое влияние в отечественной правовой науке в наши дни. Некоторые исследователи рассматривают принципы права как объективные нормы, изначально заложенные в общественных отношениях. Иногда принципы

---

[49] Демичев А.А. Позитивистская классификация принципов гражданского процессуального права Российской Федерации // Арбитражный и гражданский процесс. 2005. № 7. С. 7.; Саменкова С.Е. К вопросу о нормативном закреплении принципов права // Вектор науки Тольяттинского государственного университета. 2012. № 1 (19). С. 205.; Мутасова М.А. Проблема законодательного закрепления принципа справедливости // Социально-экономические явления и процессы. 2015. Т. 10. № 7. С. 173.

[50] Ковлакас Н.В. Нравственные основы правоприменительной практики // Вестник Таганрогского института им. А.П. Чехова. 2009. Специальный выпуск. С. 57.; Цыбулевская О.И., Милушева Т.В. Справедливость в праве: аксиологический подход // Вестник Поволжского института управления. 2017. Т. 17. № 5. С. 54.; Степаненко Р.Ф., Юн Л.В. Этические основы правоприменительной деятельности: актуальные вопросы теоретического правоведения // Вестник Казанского юридического института МВД России. 2018. № 2 (32). С. 191.

права отождествляют с «истинными нормами»[51]. Принципы права как особые категории правовой жизни общества, как продукты развитого общественного сознания могут и, безусловно, должны закрепляться в нормах права, но, вместе с тем, они могут находить в них и косвенное отражение, выводиться логическим путем из смысла и содержания действующего права. Полагаем, что отождествлять принципы права исключительно с нормами права было бы неправильно. Право формируется с учетом исторических, духовно-нравственных традиций и не может быть полностью приравнено к нормам права.

Согласно мнению С.А. Мосина, неоспоримо высокая ценность правовых принципов диктуется их фундаментальной ролью и строгой необходимостью их строгого соблюдения. Исследователь выделяет объективную природу этих принципов, подчеркивая их решающую роль и значимость в структуре правовой системы. Принципы права в российской юридической доктрине не ограничиваются рамками законодательного процесса и не сводятся исключительно к правовым нормам, они проявляются и анализируются в юридической науке как фундаментальные закономерности, которые исследуются и понимаются через научный дискурс[52].

Несмотря на тесную связь принципов права с правовыми нормами, следует отметить, что существуют ситуации, когда принципы права действуют напрямую, без посредничества норм. Такое прямое действие принципов права, например, имеет место в случаях применения аналогии права. Когда аналогия закона не может быть использована для урегулирования правового пробела, именно принципы права становятся тем инструментом, который восполняет недостатки в правовом регулировании и обеспечивает целостность правовой системы[53].

А.Н. Гасанова утверждает, что принципы российского права играют двойную роль: они помогают заполнить пробелы в законодательстве и служат источниками

---

[51] Дмитриев С.Д. К вопросу о понятии принципов права // Пробелы в российском законодательстве. Юридический журнал. 2009. № 4. С. 62.

[52] Мосин С.А. Свойства конституционных принципов // Правоприменение. 2021. № 3. С. 126-136.

[53] Климшен И. И., Нигамадзянов А.Р., Гурьянов К.А., Овод И.В. Принцип равенства участников гражданских правоотношений // Colloquium-journal. 2021. № 2. С. 35-38.

правовой системы России[54]. Тем не менее, данное мнение можно оспорить, поскольку утверждаемые принципы не в полной мере согласуются с атрибутами, которые обычно ассоциируются с источниками права[55].

Вопросы, связанные с основами правового регулирования, давно известны. Но с развитием цифровой экономики, в научных трудах начались попытки модифицировать традиционную систему норм, предложив их в видоизмененном виде[56]. Наряду с этим существует и альтернативный взгляд, согласно которому классическая система принципов, традиционно применяемая в регулировании экономических отношений, уже не может полностью удовлетворить потребности цифровой среды. В результате возникает необходимость выработки дополнительных принципов, которые бы учитывали уникальные черты и специфику новой матрицы цифровых экономических отношений[57].

Концепция, рассматриваемая в данном контексте, опирается на базовые положения, закрепленные в «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [58]. Среди ее определяющих ориентиров можно выделить обеспечение возможности граждан получать информацию, свободу индивидуального выбора способов освоения знаний, а также сохранение элементов традиционных механизмов предоставления товаров и услуг. Немаловажное значение уделяется вопросам соблюдения отечественных моральных и духовных ценностей, что находит отражение в сфере применения цифровых коммуникационных инструментов. Неотъемлемой частью выступает и приверженность принципам законности, рациональности при процессах сбора,

---

[54] Гасанова А.Н. Принципы права: современные подходы // Правовое регулирование в современной России. 2014. № 5 (44). С. 41-45.

[55] Например, отсутствует формальная определенность – прецеденты, законы обладают структурой, конкретной формулировкой и официальным закреплением. Принцип может носить абстрактный характер и может быть выражен в общей идее. Содержание будет раскрываться через толкование. Принцип не действует прямо, нельзя использовать принцип для разрешения спора без опоры на норму, также источники права санкционируются государством, а принципы вполне могут существовать на уровне доктрины.

[56] Беликов Е.Г. Развитие финансово-правовых принципов в условиях цифровой экономики // Вестник Университета имени О.Е. Кутафина. М.: МГЮА, 2020. С. 39-45.

[57] Андреева Г.Н., Бадальянц С.В., Богатырева Т.Г. и др. Развитие цифровой экономики в России как ключевой фактор экономического роста и повышения качества жизни населения: монография. Нижний Новгород: издательство «Профессиональная наука», 2018. С. 31-49.

[58] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

хранения и передачи сведений. При всем этом, меняющиеся черты общественного устройства диктуют необходимость формирования новых правовых ориентиров, способных инициировать глубокие преобразования в сфере законодательного регулирования с учетом современных представлений и мировоззрений, что должно находить свое выражение в актуализации законодательства[59].

Систематизация теоретических работ и ключевых законодательных инициатив, нацеленных на определение современных подходов к регулированию отдельных направлений цифровой экономики, свидетельствует о значительной потребности в их четкой структуризации. Формирование единых, универсальных основ правового регулирования, выступающих опорой для дальнейшего развития цифрового пространства, приобретает стратегическое значение для обеспечения устойчивого роста и создания эффективной системы правовых гарантий в Российской Федерации. Разработка таких принципов не только способствует оптимизации процессов цифровой трансформации, но и служит залогом стабильности в правовом обеспечении инновационных изменений.

Можно выделить следующие принципы:

1. Принцип законности.

2. Принцип соответствия проектируемых нормативных правовых актов стратегическим целям и задачам цифровой экономики. Разрабатываемые законодательные акты должны не только учитывать текущие потребности цифровой экономики, но и быть направленными на ее долгосрочное развитие и достижение намеченных стратегических ориентиров.

3. Принцип устойчивости правового регулирования в сфере цифровой экономики.

4. Принцип установления приоритета задействования российских организаций по обработке и хранению различных данных на территории РФ в целях обеспечения суверенитета государства. Этот принцип предусматривает необходимость обработки и хранения важных данных внутри страны, что

[59] Поляков М.П. Принцип как мировоззренческая идея относительно сущего и должного: новый подход к постижению концептуальной сущности понятия принципов отечественного уголовного процесса // Юридическая техника. 2020. № 14. С. 493-496.

укрепляет контроль государства над информационными потоками и защищает национальные интересы.

5. Принцип запрета на сокращение объема прав и свобод человека по сравнению с существовавшими до внедрения новых технологий. Здесь ключевая идея состоит в том, что внедрение новых цифровых технологий не должно ухудшать положение граждан в плане их прав и свобод. Новые подходы к правовому регулированию должны улучшать качество жизни и расширять возможности, а не ограничивать их.

6. Принцип правовой поддержки инновационных технологий. Этот принцип предполагает, что законодатель и правоприменитель активно способствуют созданию благоприятных условий для разработки и продвижения инновационных технологических решений. Он включает поддержку на всех стадиях: от идеи и исследований до коммерциализации и внедрения на рынок. Таким образом, инновации становятся не просто инструментом развития цифровой экономики, но и ее основным стимулом.

7. Принцип концептуального осознания новаторских моделей взаимоотношений участников рынка в процессе структурирования иерархии приоритетов в сфере правовой политики отражает непременность интеграции современных подходов и концепций в динамике рыночных отношений. Данный принцип подчеркивает объективную необходимость для правовой теории и законодательной практики принимать во внимание мировоззренческие сдвиги, происходящие на фоне цифровизации общества. В его основе лежит осознание того, что правовое регулирование должно отражать и поддерживать фундаментальные сдвиги в принципах взаимодействия участников рынка.

8. Принцип комплексного правового регулирования информационных отношений заключается в том, что правовая политика должна распространяться на множество аспектов социальных взаимодействий, охватывая не только экономические связи, но и прочие формы общественной жизни, которые тесно переплетены с экономической активностью. Таким образом, подход к правовому регулированию становится более целостным, что позволяет обеспечить

согласованность и эффективность норм, регулирующих различные стороны цифровой экономики.

9. Принцип ограниченной правовой децентрализации вводит приоритет диспозитивного и рекомендательного регулирования, сорегулирования и саморегулирования.

10. Целью принципа равноправного доступа экономических агентов к цифровой инфраструктуре является обеспечение возможности для всех участников экономической деятельности, включая представителей малого и среднего бизнеса, а также конечных потребителей, активно участвовать в цифровой экосистеме.

11. Принцип альтернативности цифровым инновациям подразумевает сохранение права выбора формы взаимодействия. Участники рынка и потребители сохраняют возможность использовать как цифровые, так и традиционные методы коммуникации, что предотвращает принудительный переход к новым технологиям и обеспечивает более плавную адаптацию к цифровым изменениям.

12. Суть принципа правовой стандартизации состоит в формировании и реализации системы нормативных актов, определяющих обязательные требования в ключевых областях цифровой экономики, таких как этика цифрового взаимодействия, стандарты занятости в новых технологических условиях и другие регулятивные положения. Введение таких стандартов обеспечивает единообразие юридической практики, создает прозрачные и справедливые условия функционирования для всех субъектов цифрового рынка, а также способствует предотвращению правовой неопределенности и снижению числа конфликтных ситуаций.

13. Доктринальная легитимация в сфере правовой политики ориентирована на то, чтобы процесс всего законотворчества предусматривал обязательную экспертную проверку вводимых актов. В рамках такого подхода значительное участие принимают представители делового сектора и профессионального сообщества, которые рассматривают целесообразность, действенность и возможные ограничения принимаемых правовых инноваций, а также сопоставляют оптимальные сроки их реализации. Благодаря такому

механизму формируется основа для разработки правовых положений, находящих общественное признание и обеспечивающих гармоничный баланс интересов различных социальных групп.

14. Свобода выбора при приобретении цифровых товаров и услуг предполагает закрепление нормативных гарантий, позволяющих пользователям самостоятельно определять перечень дополнительных сервисов и контента. В законодательстве предусматривается, что производители цифрового оборудования и разработчики платформ обязаны создавать условия, при которых потребителям предоставляется возможность выбирать и использовать программные продукты, соответствующие установленным критериям безопасности. При этом создатели цифровых решений получают законное основание размещать на платформах любые разработки, которые удовлетворяют этим стандартам, тем самым обеспечивается баланс интересов пользователей и разработчиков, а также поддерживается конкуренция и инновационное развитие в цифровой экономике.

15. Превентивное регулирование в сфере экономических взаимоотношений, связанных с применением современных технологий, исходит из требования учитывать вероятные угрозы, возникающие в процессе цифровизации. Усиление темпов цифрового преобразования экономики в последние годы стимулировало разработку подходов, позволяющих выдвигать и применять упреждающие меры. Среди них особое место занимает использование методик юридического моделирования общественных процессов, а также проведение правового прогнозирования, благодаря чему становятся возможными формулирование и введение нормативов, предотвращающих возникновение проблем еще до их фактической реализации. Такой подход поддерживает устойчивость правовой среды и минимизирует негативные последствия внедрения инновационных решений.

16. Принцип обеспечения инфраструктурно-технологического суверенитета предполагает последовательную разработку нормативных актов, направленных на развитие отечественных аналогов сложных технических устройств и программного обеспечения. Этот принцип ориентирован на системное

и поэтапное формирование нормативной базы, способствующей снижению зависимости от зарубежных технологий и повышению технологической независимости страны[60].

В науке принципы классифицируются по нескольким основаниям.

Комплексный характер настоящего исследования предполагает адаптацию классификации принципов-методов, раскрывающих сущностные основы информационно-правового обеспечения, которые не должны противоречить базовым принципам. В качестве модели рассматривается классификация, предложенная А.А. Волосом, который подразделяет принципы-методы на несколько групп[61]:

– принципы, обеспечивающие свободу и частную автономию участников оборота, которые направлены на создание нормативной среды, где субъекты могут действовать свободно, в рамках установленных законом норм, самостоятельно определяя содержание своих отношений и принимая решения, исходя из личных интересов и предпочтений;

– принципы, формирующие механизмы соблюдения равенства субъектов оборота. Предусматривают установление таких правовых средств, которые гарантируют равные возможности и условия для всех участников экономического оборота, вне зависимости от их размера, организационно-правовой формы или положения на рынке;

– позволяющие осуществить оценку поведения субъектов. Включают правовые нормы и подходы, обеспечивающие возможность объективной оценки действий сторон, а также применения санкций или поощрений на основе ясных и заранее установленных критериев;

– принципы, составляющие основу для соблюдения прав и их защиты. Это группа принципов направлена на создание эффективных механизмов защиты

---

[60] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. М.: Фонд развития центра разработки и коммерциализации новых технологий, 2020. 32 с.

[61] Волос А.А. Система принципов-методов гражданского права: постановка проблемы // Ленинградский юридический журнал. 2016. № 3. С. 97-98.

законных интересов участников оборота, восстановление нарушенных прав, а также обеспечение справедливого разрешения споров.

Такая классификация отражает ключевые характеристики, которыми должны обладать принципы в рассматриваемой области. Они формируют прочный фундамент для разработки нормативных правовых актов, регулирующих информационные отношения, и служат гарантией их устойчивости и предсказуемости.

Развитие цифровой экономики вносит существенные коррективы в основополагающие начала гражданского оборота. Среди принципов, подвергающихся изменениям, значимую роль играет свобода заключения договоров, хотя иногда ее осуществление может вступать в противоречие с требованиями законодательных актов. Кроме того, акцентируется внимание на защите права и его восстановлении после нарушений; не менее важным представляется принцип добросовестности, играющий центральную роль в механизме восстановления прав, оказавшихся ущемленными[62].

К другой группе принципов можно отнести:

– принцип электронного документооборота;

– принцип равновесного защиты конфиденциальных данных и коммерциализации информации;

– принцип цифрового императива[63];

– принцип «цифрового легалитета» (т.е. признанные цифровые права на цифровые объекты, подтверждающиеся записями в информационной системе)[64];

– принцип технологической нейтральности. Основополагающие принципы не дискриминации, технологической нейтральности были

[62] Волос А.А. Смарт-контракты и принципы гражданского права // Российская юстиция. 2018. № 12. С. 5-7.

[63] Карцхия А.А. Гражданско-правовая модель регулирования цифровых технологий: дис. … д-ра юрид. наук: 12.00.03. М., 2019. С. 244-245.

[64] Ворникова Е.Д. Правовое регулирование внешней торговли услугами в цифровой экономике: дис. … канд. юрид. наук: 5.1.3. М., 2023. С. 99.

задекларированы в Типовом законе об электронных подписях ЮНСИТРАЛ 2001 года (ст. 3) и п. 82 Руководства по принятию[65].

Необходимо отметить, что принцип технологической нейтральности широко применяется в технологической сфере. В частности, этот принцип закреплен в п. 2 ст. 434 Гражданского кодекса Российской Федерации, который позволяет использовать любые технологии для обмена документами, если эти технологии способны подтвердить факт получения документа от контрагента по договору. Кроме того, принцип технологической нейтральности находит выражение в возможности защиты авторских прав с помощью технологий, контролирующих доступ к информации, что закреплено в ст. 1299 ГК РФ.

В современном мире информационные технологии занимают ключевую позицию в формировании направлений развития не только в технологическом аспекте, но и в экономическом и социальном контекстах. Цифровые инновации могут быть рассмотрены как некий катализатор современности, выступая в виде существенного норматива общественного значения. Этот норматив возникает на фундаменте характеристик цифровой среды и целенаправленно стремится к обновлению принципов работы и взаимодействия в разнообразных областях жизнедеятельности населения.

Принцип цифрового императива А.А. Карцхии представляет собой совокупность подходов к правовому регулированию цифрового гражданского оборота, формирующих направленность адаптации законодательства к условиям цифровой экономики. Этот принцип включает разработку и внедрение системы норм, касающихся цифровых прав, цифровых объектов, субъектов этих прав, а также механизмов их реализации, защиты и правоприменения[66].

В современном мире растет значимость цифровой экономики и, как следствие, возникает необходимость в регулировании отношений в сфере цифровых прав. Это новое направление, пронизывающее гражданский оборот,

---

[65] Типовой закон ЮНСИТРАЛ об электронных подписях и Руководство по принятию 2001 г. ООН, Нью-Йорк, 2002 // URL: https://www.uncitral.org/pdf/russian/texts/electcom/ml-elecsig-r.pdf.

[66] Карцхия А.А. Гражданско-правовая модель регулирования цифровых технологий: дис. … д-ра юрид. наук: 12.00.03. М., 2019. С. 244-245.

требует внимания законодателя для организации эффективного взаимодействия участников цифровой среды.

Учитывая формирование специфических отношений, возникает вопрос: достаточно ли имеющегося методологического воздействия для регулирования нового? Можно попробовать подтверждать права по аналогии с институтом интеллектуальной собственности (применять меры защиты, принцип израсходования имущественного права).

По аналогии с международным принципом торговли lex mercatoria, правовое регулирование отношений в сфере информационных технологий требует унификации, что предполагает согласование национальных правовых систем и опору на сложившуюся практику их применения. Создание новых оснований и подходов к правовому управлению в сфере гражданских взаимоотношений на фоне использования информационных технологий, известное как «цифровой императив», закладывает концептуальную базу для прогресса цифровой экономики. Это связано с потребностью приведения правовых стандартов в соответствие с новой технологической реальностью и изменениями в правовом управлении, что, в свою очередь, стимулирует создание новой модели развития правопорядка.

В рамках категории «цифрового императива» учитываются не только общие принципы гражданского права, но и ряд специальных принципов, которые соответствуют особенностям цифрового гражданского оборота. Среди них можно выделить принципы технологической нейтральности, анонимной аутентификации, устойчивости цифрового оборота и другие, которые были ранее обозначены. Все они создают основу для выработки новых подходов к правовому регулированию, обеспечивая адаптацию гражданских правоотношений к условиям цифровой среды.

В дополнение к общим и ранее обозначенным принципам цифрового гражданского оборота целесообразно выделить следующие ключевые подходы, связанные с его построением и функционированием:

– принцип «цифровой законности» подразумевает процесс проверки (утверждения легитимности) цифровых прав на цифровые активы, которые заверены с помощью цифровых кодов внутри электронных регистров;

– принцип криптошифрования способа передачи данных и ведения реестров записей. В его основе лежит применение криптографических технологий для защиты данных, передаваемых между субъектами цифрового оборота, а также для обеспечения надежности и непротиворечивости информации, хранящейся в реестрах;

– принцип устойчивого обмена информационными потоками. Он ориентирован на создание правовых и технологических условий для стабильного и непрерывного обмена информацией между участниками цифрового оборота. В его рамках разрабатываются механизмы, позволяющие избежать перебоев в обмене данными, обеспечить доступность информации в любой момент и снизить риски потери данных.

Цифровизация экономики несет в себе двойственный характер изменений. С одной стороны, она вызывает ревизию традиционных принципов, обновляя их сущность. С другой стороны, она инициирует формирование совершенно новых принципов. Адаптация к новым реалиям также подразумевает расширение толкования этих принципов. Это может выражаться в равноправном узнавании электронных объектов наряду с традиционными физическими, а также в применении к ним существующих норм и правил[67].

К числу основополагающих принципов, которые оказались под воздействием цифровой экономики, можно отнести следующие: автономия волеизъявления сторон в договорных отношениях, обеспечение и возмещение ущерба при нарушении прав, принцип добросовестности и предоставление защиты менее защищенной стороне[68].

---

[67] Романенкова Е.И., Шведчиков А.В. Интеллектуальная собственность. Обзор событий в России и за рубежом (второе полугодие 2016 г.) // СПС «КонсультантПлюс» (дата обращения 02.02.2025). URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=101555#JKGVdpUuKfSxIz15.

[68] Волос А.А. Смарт-контракты и принципы гражданского права // Российская юстиция. 2018. № 12. С. 5-7.

Процесс цифровизации расширяет инструментарий для оформления сделок, предоставляя участникам новые технические возможности. Однако утверждения о необходимости трансформации базового принципа свободы договора на данном этапе могут быть преждевременными. В контексте традиционного понимания права, данный принцип включает в себя элементы, такие как свобода выбирать партнера по сделке, способ ее осуществления и детали договоренности. Однако использование блокчейн-технологий в виде смарт-контрактов и анонимных операций порождает новые опасности для устойчивости гражданских правоотношений. Невозможность достоверно идентифицировать контрагента ведет к утрате перспектив обращения в судебные инстанции для защиты своих прав и сужает возможности получения информации до заключения договорных отношений. Это означает, что несмотря на расширение возможностей выбора, стороны сделок сталкиваются с новыми правовыми и техническими рисками, которые они должны учитывать при принятии решения о заключении соглашения[69].

Принцип обеспечения восстановления нарушенных прав в правоотношениях, в которых присутствует виртуальный объект, подталкивает к внедрению концепции права доступа, так как иных средств защиты не существует[70]. Учитывая специфику отношений, участники оборота нуждаются в применении механизмов самозащиты.

Принцип свободы договора, действительно, может быть применен к отношениям с использованием смарт-контрактов. Однако это не требует изменения самого принципа. Субъекты, вступающие в договорные отношения на основе самоисполняющихся контрактов, сохраняют возможность защиты своих прав в судебном порядке, если выявляются дефекты в структуре или содержании контракта. Таким образом, использование смарт-контрактов лишь расширяет технические способы реализации договорных условий, но не отменяет базовых

[69] Ковалева Н.Н. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций (научный обзор) / Н.Н. Ковалева, Н.А. Жирнова // Информационное право. 2024. № 1 (79). С. 40.

[70] Кирсанова Е.Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: дис. … канд. юрид. наук: 12.00.03. М., 2021. С. 188.

правовых гарантий и не требует пересмотра принципиальных основ договорного регулирования. Но, с учетом принципа защиты слабой стороны, можно предположить об установлении ограниченного перечня сфер общественной жизни, в котором можно использовать смарт-контракт (ограничиться сферами, где участвуют потребитель и поставщики услуг, например, продажа первичного жилья).

Говоря про новые принципы, можно указать на то, что для установления эффективного оборота и развития цифровой экономики область правового регулирования нуждается в создании системы принципов, которые позволили бы внедрить технологии без ущерба.

В качестве новых принципов, с учетом которых необходимо формировать информационно-правовое обеспечение цифровой экономики, можно предложить:

1. Принцип координирующего информационно-правового воздействия предполагает целенаправленное регулирование развития как экономических, так и связанных с ними общественных отношений. Это правовое воздействие должно быть направлено на упорядочение процесса эволюции данных отношений, особенно с учетом растущего числа правонарушений в цифровой среде. Он включает в себя меры, способствующие предотвращению нарушений, поддержанию стабильности и защите прав субъектов в условиях цифровой трансформации.

2. Принцип международной согласованности ориентирован на создание согласованных моделей правовой политики, которые способствуют установлению единых правил для экстерриториальной цифровой экономики. Требует разработки правовых стандартов, которые могли бы применяться в различных юрисдикциях, обеспечивая правовую гармонизацию, снижение юридических барьеров для международного цифрового взаимодействия и более эффективное решение трансграничных споров.

3. Развивая положения принципа 12 из Концепции[71] в более прикладной призме, можно сформулировать принцип обеспечения прозрачности использования алгоритмов и моделей искусственного интеллекта, а также осведомленности пользователей при взаимодействии с ними.

4. Продолжая проблематику внедрения искусственного интеллекта, необходимо развивать данное направление с учетом принципа осознанного замедления внедрения технологии искусственного интеллекта, так как право всегда вторично, необходимо быть адаптированным в момент широкого внедрения искусственного интеллекта.

5. Принцип всеохватывающего бездокументарного взаимодействия в электронной форме. Принцип декларирует взаимодействие в электронной форме, распространение смарт-контрактов, предоставление государственных услуг в электронной форме и тому подобное. Необходимо указать на тот факт, что действующее законодательство допускает заключение сделок с электронной подписью, следовательно, вопрос о литеральной форме на бумаге не стоит[72].

6. Принцип информационной идентификации, под которым предлагается понимать необходимость установления юридической принадлежности информации и прав на ее обработку соответствующим субъектам цифровой экономики. Данный принцип сочетает в себе факт идентификации субъекта и связанную с ним обязанность третьих лиц по недопущению нарушений прав и законных интересов данного субъекта, возникающих при разглашении принадлежащей ему информации и результатов идентификации, алгоритмов и способов такой идентификации[73].

7. Правовая интероперабельность, представляющая собой способность к налаженному информационному взаимодействию, предусматривает, что государственные органы и участники хозяйственной деятельности не только

---

[71] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. М.: Фонд развития центра разработки и коммерциализации новых технологий, 2020. 32 с.

[72] Гайдаенко Ш.Н., Грачев Д.О., Лещенков Ф.А. и др. Договоры в гражданском праве зарубежных стран: монография / отв. ред. С.В. Соловьева. М.: ИЗиСП, НОРМА, ИНФРА-М, 2018. 336 с.

[73] Рустамов П.А. Принципы информационно-правового обеспечения цифровой экономики // Евразийская адвокатур. 2024. № 5 (70). С. 193.

обладают полномочиями, но и несут ответственность за координированный обмен информацией и знаниями. Такой обмен происходит согласно установленным регламентам и в обозначенных рамках, не встречая препятствий, связанных с доступом или применением полученных данных. Данная концепция формирует фундамент для развития цифрового управления, интегрированного в государственную политику в условиях цифровой экономики, а также играет ключевую роль при создании единого цифрового пространства для эффективной работы цифрового рынка[74].

§ 1.2. Объекты информационно-правового обеспечения цифровой экономики

Информационные отношения возникают, претерпевают изменения и прекращаются в рамках информационной сферы, где их регулирование осуществляется с помощью норм информационного права. Это означает, что правовые нормы, относящиеся к информационному праву, устанавливают правила и принципы, которые должны соблюдаться участниками информационных отношений, обеспечивая таким образом стабильность, предсказуемость, а также защиту прав и интересов всех субъектов этих отношений[75].

Объектами информационного правоотношения являются разнообразные материальные, духовные и социальные ценности, а также действия и продукты творческой деятельности, которые становятся предметом информационных правоотношений. Эти объекты составляют основу интересов, прав и обязанностей участников информационных отношений. Материальные объекты информационного правоотношения могут включать различные виды информации: документы, базы данных и другие материальные средства, используемые для создания, обработки, хранения и распространения информации. Например,

---

[74] Рустамов П.А. Принцип правовой интероперабельности как связующий элемент формирования нормативного ландшафта экономики в условиях цифровизации // Евразийская адвокатура. 2025. № 2 (73). С. 165-170.

[75] Амиржан К.Ж. Информационные правоотношения: общетеоретический аспект // Вестник Омского университета. Серия: Право. 2017. № 1 (50). С. 31-35.

авторские произведения, такие как книги, фильмы или музыкальные композиции, могут быть объектами информационных правоотношений, когда авторы предоставляют права на использование своих произведений другим лицам. Нематериальные объекты информационного правоотношения включают идеи, знания, информацию, которые могут быть предметом обмена, использования и защиты в информационных отношениях. Например, научные открытия, технические разработки или интеллектуальные концепции могут быть объектами информационных правоотношений, когда их создатели получают права на использование их результатов. Социальные блага, такие как информация о политической, экономической, социальной или культурной сфере, также могут быть объектами информационных правоотношений. Например, государственные органы предоставляют информацию о нормативных правовых актах, правилах и политиках, которые становятся объектами информационных правоотношений между государством и гражданами.

Объектами информационных правоотношений могут быть действия и воздержание от действий. Например, запрет на распространение определенной информации или требования к предоставлению информации могут стать объектами информационных правоотношений в том случае, когда субъекты рассматриваемых правоотношений обязаны соблюдать эти требования или ограничения.

Объекты творческой деятельности, к числу которых относятся произведения авторского права, патенты на технические решения и зарегистрированные товарные знаки, определяются в качестве составляющих информационных правоотношений. Правообладатели наделены возможностью передавать другим лицам полномочия по использованию своих интеллектуальных продуктов, одновременно устанавливая соответствующие ограничения и правила эксплуатации этих объектов[76].

[76] Ковалева Н.Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта / Н.Н. Ковалева, Н.А. Жирнова // Журнал российского права. 2024. Т. 28, № 7. С. 109.

Таким образом, объекты информационного правоотношения охватывают широкий спектр общественных отношений, затрагивающих различные сферы материальных, духовных и социальных благ. Эти отношения становятся предметом регулирования информационного права и определяют интересы, права и обязанности участников таких правоотношений.

Вопросы классификации объектов информационных правоотношений практически не затрагиваются в рамках современных исследований. В процессе классификации элементов информационно-правовой поддержки цифровой экономики анализируются объекты, связанные с правовыми отношениями, включая данные и информационные активы, информацию, информационные структуры, услуги в сфере информации и соответствующие операции, в частности технология искусственного интеллекта, осуществление сделок в цифровой среде, особенности финансовых отношений в цифровую эпоху и ряд других.

Согласно позиции В.А. Копылова, основным объектом информационных правоотношений является информация[77]. Данная категория достаточно подробно изучена в рамках различных направлений научных исследований и можно выделить базовые подходы к определению рассматриваемого термина[78].

С.Н. Шевердяев акцентировал внимание на том, что объем и многообразие исследований в области информации и информационных процессов крайне велик, а научное определение понятия «информация» окончательно не выявлено. Тем не менее данное обстоятельство не мешает в собственно юридических исследованиях разрабатывать вопросы регулирования общественных отношений по поводу информации. Подобно другим социальным отраслям знания для правовой науки важными являются факты и закономерности в области информационных процессов и эффектов в обществе[79].

---

[77] Копылов В.А. Информационное право: учебник - изд. 2-е, перераб. и доп. - М.: Юристъ, 2004. 512 с.

[78] В качестве примеров, подтверждающих тезис о широте исследуемой категории и ее многогранности в правовых исследованиях, можно привести работы Авакьяна С.А. Задачи конституционного права в аспекте защиты (от) информации. 2022. № 8. С. 3-11.; Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации: дис. … д-ра. юрид. наук: 12.00.03. — Моск. гос. юр. академия, Москва, 2007. 422 с.

[79] Шевердяев С.Н. Проблемы конституционно-правового регулирования информационных отношений в Российской Федерации: дис. ... канд. юрид. наук: 12.00.02. М., 2002. С. 13.

Классический подход, сформированный в основном западными авторами, такими как К. Шенон и У. Уивер, рассматривает информацию как данные, факты или знания, которые передаются и используются для принятия решений или получения определенного знания[80]. В рамках данного подхода информация рассматривается как объективное явление, отделенное от субъектов и контекста.

Информация рассматривается как знаки и символы, которые передают определенное значение или сообщение исследователями, принадлежащими к семиотическому направлению, представителями которого является такие авторы, как У. Эко[81] и Р. Барт[82]. В рамках семиотического подхода информация воспринимается как процесс коммуникации, где смысл передается от отправителя к получателю.

Согласно конструктивистскому подходу, информация рассматривается как результат взаимодействия субъекта и окружающей среды, вследствие чего создается и интерпретируется субъектом на основе его представлений, опыта и контекста. Данный подход акцентирует роль активности субъекта в процессе создания и восприятия информации.

Прагматический подход изучает информацию с точки зрения ее полезности и применимости для достижения определенных целей, оценивая информацию на основе ее ценности и эффективности в конкретном контексте[83].

Выделение формально-определенных и содержательных признаков информации, предложенное И.М. Рассоловым, является важным для более глубокого понимания. Первый признак, выделенный автором, заключается в том, что сообщение и данные являются независимыми от формы их представления. Независимость от формы представления позволяет информации быть гибкой и адаптивной к различным средам и технологиям. Например, информация может

---

[80] Shannon C.E., Weaver W. The Mathematical Theory of Communication. University of Illinois Press. 1949. 125 p.

[81] Eco U. Semiotics and the philosophy of language. Bloomington: Indiana University Press, Midland Book Edition. 1986. 256 p.

[82] Barthes R. Elements of Semiology / Transl. by A. Lavers, C. Smith. N.Y.: Hill and Wang, 1982. 128 p.

[83] Воройский Ф.С. Информатика. Новый систематизированный толковый словарь-справочник (Введение в современные информационные и телекоммуникационные технологии в терминах и фактах). М.: ФИЗМАТЛИТ, 2003. 760 с.

быть передана через печатные материалы, электронные документы, интернет-сайты, социальные сети и другие каналы связи. Второй предложенный признак связан с рассмотрением информации через категорию «сведения», в рамках которой информация трактуется как отражение данных в человеческом сознании на уровне мыслительной деятельности. Это означает, что информация получает смысл и ценность благодаря способности человека воспринимать, интерпретировать и использовать данные. Информация становится сведениями, когда она воспринимается и обрабатывается человеком, что позволяет использовать ее для принятия решений, получения знаний и коммуникации.

Понимание этих признаков информации имеет важное значение для разработки правовых норм и политик, связанных с информацией. Например, при регулировании передачи информации через различные каналы связи и платформы, необходимо учитывать ее формально-определенные признаки, чтобы обеспечить ее целостность и достоверность. Содержательные признаки информации также могут быть учтены при разработке политик в области защиты данных, прав доступа к информации и интеллектуальной собственности[84].

В рамках данного исследования под информацией, как объектом информационных правоотношений, рассматриваются цифровые данные, факты, знания, контент и цифровые активы, которые имеют юридическую значимость и используются в рамках информационных правоотношений. Информация, как объект информационных правоотношений, может быть представлена в различных форматах, включая текст, изображение, аудио- и видеофайлы, базы данных и тому подобное.

В цифровой экономике информация является одним из основных ресурсов и активов, которые обладают стоимостью и способны создавать экономическую ценность, используется для передачи знаний, принятия решений, совершения сделок, предоставления услуг и других целей. Также информация в цифровой экономике является объектом правовой защиты. Правовая защита информации

[84] Рассолов И.М. Информационное право: учебник для магистров. М.: Изд-во Юрайт, 2015. 444 с.

обеспечивает создателям и владельцам информации права на ее использование, контроль за распространением и защиту от незаконного использования.

В научном труде Г.А. Шокирова, освещается идея о том, что уникальные характеристики и правовой режим информации находят свое выражение через информационные системы и процессы. Эти системы и процессы играют ключевую роль в осуществлении основополагающих прав на информацию, которые закреплены в основном законе страны, и в обеспечении выполнения обязательств ответственными лицами для поддержки данных прав и свобод. Это утверждение подчеркивает важность информационных процессов в правовом регулировании, а также роль информации как важного элемента в системе защиты прав граждан[85].

Анализ тематики, связанной с объектами информационного права, требует углубленного изучения таких составляющих, как массивы данных, которые формируются с помощью программ, использующих алгоритмы машинного обучения. Согласно статье 5 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация утверждена в роли составляющей гражданско-правовых отношений[86].

Тем не менее, в контексте существующего разногласия между нормами федеральных законов и положениями ГК РФ, следует осознавать, что информация не получила режим обособленного имущественного объекта. Она отсутствует в перечне статьи 128 ГК РФ, где определены виды имущества. Это создает определенную правовую неопределенность и представляет потенциальные трудности в правоприменительной практике, особенно в вопросах признания прав собственности в цифровой среде.

Особое внимание заслуживает тот факт, что информационные ресурсы, в том числе те, что созданы и обрабатываются с помощью искусственного интеллекта, становятся все более ценными в цифровом обществе. С учетом этого появляется

---

[85] Шокиров Г.А. Информация как основной объект информационных правоотношений: теоретический и практический аспекты // Вестник Томского государственного университета. 2017. № 415. С. 212–216.

[86] Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5-18.

необходимость переосмысления и уточнения нормативной базы, регулирующей режим информации, ее защиту и использование в различных сферах деятельности.

Как указывалось выше в диссертационном исследовании, существуют разные подходы к сущностному наполнению категории «информация», которое прямо коррелирует со спецификой отношений.

Так, например, если мы обращаемся к защите чести и достоинства граждан и юридических лиц, информация будет синонимична «сведениям», хотя, учитывая определение информации из Закона об информации, оно включает категорию сведения. Термин «информация» может использоваться для обозначения как цифровых данных, так и элементов баз данных, которые подлежат защите.

Стоит подчеркнуть, что при нарушении условий соглашения о конфиденциальности, и последующем раскрытии информации, возникают проблемы с признанием этой информации в качестве полноценного объекта правовой защиты. В таких обстоятельствах обычно дело сводится не к восстановлению нарушенного правового режима информации, а к вопросам возмещения причиненных потерь. Реализация мер по компенсации нанесенного ущерба зачастую оказывается более релевантной, нежели применение механизмов защиты информации, как таковой, в юридической плоскости.

В академическом сообществе проводится дискуссия о режиме информации, предлагается ее рассмотрение как независимого объекта гражданских правовых отношений. Е.Н. Насонова исходит из убеждения, что эволюция общественных отношений и возросшая значимость информации как средства влияния на экономические связи и правовую сферу обуславливают ее выделение в отдельную категорию. Особо подчеркивается, что в эпоху цифровизации, информация приобретает особенности ключевого ресурса и оказывает прямое воздействие на многообразные аспекты деятельности человека, стимулируя тем самым обновление подходов к ее правовому регулированию[87].

[87] Насонова Е.Н. Информация как объект гражданского права: дис. … канд. юрид. наук: 12.00.03. М., 2002. С. 13-14.

Е.А. Суханов полагает, что самостоятельным объектом гражданских прав информацию считать невозможно. В его трактовке информация предстает как философское понятие, и лишь та ее часть может пользоваться охраной, которая наделена признаками, позволяющими рассматривать ее как объект имущественных интересов. Только когда информация приобретает экономическую ценность и отвечает установленным критериям, возможно ее признание защищаемым объектом в рамках действующего правового регулирования[88].

Получается для выделения информации как объекта гражданских прав необходимо выполнение следующих требований:

– должна быть эвентуальность ее объективизации;

– данные должны быть экономически ценными.

Информационные системы выступают следующей наиболее крупной категорией.

Информационные системы и их компоненты, в том числе базы данных, библиотеки, архивы, являются важными объектами информационно-правового обеспечения цифровой экономики. Понятие информационной системы выходит за рамки исключительно базы данных, но также охватывает более обширные физические активы, в числе которых находятся разнообразные системы, задействованные в процессах сбора, сохранения, обработки и распространения информации.

На глобальной арене термин «информационная система» получил свое определение в рамках Конвенции, принятой под эгидой Организации Объединенных Наций 23 ноября 2005 года. В соответствии с указанным международным актом, информационные системы описываются как сформированные структуры, задействованные для манипулирования информационными потоками, что включает процессы приема, пересылки и архивирования сообщений и данных. Эти операции являются ключевыми для

[88] Перспективы развития гражданского законодательства в России: планы и современные реалии [Интервью с Е.А. Сухановым] // СПС «КонсультантПлюс» (дата обращения: 20.01.2025).

обеспечения циркуляции и сохранности информации в современном инфопространстве[89].

В контексте законодательства Европейского Союза концепция информационной системы охватывает комплекс технических устройств, задействованных для автоматизированного процесса датапроцессинга. При этом данные подлежат обработке и передаче через эти устройства. В соответствии с положениями регламента Европейского союза, под информационной системой понимается либо отдельное техническое средство, либо совокупность взаимосвязанных устройств. Определенные элементы такой системы функционируют в автоматическом режиме, обрабатывая большие объемы информации по заложенным программам. Важным составляющим компонентом рассматриваемых систем выступают данные, операции с которыми — такие как хранение, обработка, поиск и передача посредством названных устройств — направлены на поддержание стабильной работы, эффективного использования, высокоуровневой защиты и корректного обслуживания всей системы[90].

Согласно Модельному закону «Об информации, информатизации и обеспечении информационной безопасности», утвержденному Межпарламентской Ассамблеей государств — участников СНГ, под информационной системой следует понимать совокупность взаимосвязанных средств, предназначенных для выполнения определенных технологических функций. Такие системы реализуют процессы обработки информации с целью выработки решений, необходимых для решения поставленных задач[91].

Вместе с тем, сформулированное выше определение существенно ограничивает представление об информационной системе, поскольку не учитывает ее содержательную комплексность и акцентирует внимание лишь на

---

[89] Конвенция ООН об использовании электронных сообщений в международных договорах. Принята резолюцией 60/21 Генеральной Ассамблеи от 23 ноября 2005 года. URL: https://www.un.org/ru/documents/decl_conv/conventions/elect_com.shtml.

[90] Директива Европейского парламента и Совета Европейского Союза 2013/40/ЕС от 12.08.2013. Об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД Совета ЕС. Текст официально опубликован не был.

[91] Об информации, информатизации и обеспечении информационной безопасности: Модельный закон. Приложение к постановлению МПА СНГ от 28.11.2014 г. № 41-15.

инструментальной стороне, что нередко приводит к отождествлению системы исключительно с базой данных. В результате оказывается незамеченной роль информационной системы в более широких процессах и процедурах обработки, передачи и использования информации.

В российских правовых актах данное понятие имеет официальное толкование, закрепленное в федеральном законе, регламентирующем вопросы обращения информации, применение информационных технологий и обеспечение ее безопасности[92].

В федеральном законе, регламентирующем вопросы обращения и защиты данных, информационная система трактуется как объединение сведений, размещенных в базах данных, а также технических и программных ресурсов, обеспечивающих их обработку. Совокупность информации и методов ее преобразования формирует теоретическую базу для глубокого анализа и многообразного использования информационных систем в различных сферах.

Развернутое толкование включает в себя не только аспекты хранения критически важных данных, но и указывает на комплексный набор процедур, процессов и методик, используемых для взаимодействия с данными. При этом неотъемлемым элементом является инфраструктура, состоящая из программного и аппаратного обеспечения, что в совокупности образует экосистему для циркуляции и защиты информации.

Такое широкое и детализированное прочтение позволяет не просто точно описать систему, но и обеспечивает комплексное понимание ее роли в информационном пространстве, акцентируя внимание на ее важности в современном цифровом мире.

Г.Л. Акопов в своей работе подчеркивает, что основное предназначение информационной системы заключается в реализации информационных процессов в области ее функционирования, что акцентирует важность информационной

[92] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

системы как инструмента для эффективного управления данными и их обработки в различных сферах деятельности[93].

В истории научного дискурса интенсивно велись дебаты относительно разграничения понятий «информационные системы» и «системы информационного обеспечения». Первоначально, термин «информационные системы» относился к комплексным, хорошо организованным структурам, которые были способны выполнять широкий спектр операций с информацией, включая ее прием, сохранение, обработку, распространение и применение. В контрасте с этим системы информационного обеспечения воспринимались как инструментарий, предназначенный для поддержки информационных потребностей обширных корпоративных структур[94].

С годами в жизнь ввелись и стали привычны выражения, такие как «информационно-поисковые системы» и «системы визуализации информации», которые отражали эволюцию и усовершенствование в данной области. В последствии, с учетом новации в технологической сфере, применяется также понятие справочно-правовых систем, что еще больше расширяет границы понимания информационных систем, позволяя глубже анализировать их функциональные возможности. Это, в свою очередь, отражает прогресс восприятия и классификации информационных потоков и способов работы с ними[95].

Постепенно понятие «информационные системы» вышло за рамки сугубо алгоритмических комплексов, охватив в своем содержании не только механизмы обработки, но и сам информационный компонент, интегрированный в структуру системы. Такое расширение интерпретации связано с эволюцией технологий и переходом к более многоуровневому пониманию функционала подобных систем. В научных публикациях, посвященных анализу сущности информационных систем, отмечается, что информация определяется как совокупность сведений о реальности, уменьшающая неопределенность знаний субъекта. Обычно такие сведения фиксируются в форме сообщений, доступных для воспроизведения, что

---

[93] Акопов Г.Л. Информационное право: учебное пособие. Ростов н/Д: Феникс, 2008. С. 67.
[94] Лопатин В.Н. Информационная безопасность России: дис. … д-ра юрид. наук: 12.00.01. Спб., 2000. С. 274.
[95] Лопатин В.Н. Указ. соч. С. 275.

подчеркивает их значение как инструмента для повышения определенности и углубления познания[96].

Каждая информационная система подлежит анализу с точки зрения семантики, что влечет за собой изучение содержания и значимости информации в рамках данной системы. А.В. Минбалеев предоставил наиболее точное объяснение семантического аспекта информации, описывая ее как идеальный результат отображения мира вокруг нас, который охватывает все его элементы (феномены, объекты, процессы, отношения), и который имеет свою определенную форму восприятия объективной реальности[97].

Л.К. Терещенко предлагает классифицировать информацию как две разновидности благ: экономические и неэкономические. Под экономическим благом понимается применение информации в рамках частного права, где она выступает инструментом для реализации личных амбиций, таких как извлечение прибыли и достижение коммерческой успешности.

В отличие от экономических благ, неэкономические ценности относятся преимущественно к сфере публичного права и ориентированы на улучшение качества жизни граждан, а также на обеспечение приоритета интересов общества и государственных институтов. Информационный ресурс становится важнейшим фактором реализации задач с выраженной социальной значимостью, а также инструментом, способствующим сохранению и защите законных интересов как отдельных граждан, так и общества в целом[98].

Однако, как отмечает Л.К. Терещенко, «не вся информация сохраняет свою ценность при ее распространении». С экономической точки зрения информация обладает такими характеристиками, как новизна, определенная степень распространенности и другими свойствами, что позволяет относить ее к категории

---

[96] Трутнев Д.Р. Архитектура информационных систем. Основы проектирования: учебное пособие. Спб.: НИУ ИТМО, 2012. С. 8.

[97] Минбалеев А.М. Система информации: теоретико-правовой анализ: дис. … канд. юрид. наук: 12.00.14. – Челябинск, 2006. С. 32.

[98] Терещенко Л.К. Модернизация информационных процессов и информационного законодательства. [Электронный ресурс]. Режим доступа: СПС «Консультант Плюс».

частных благ[99]. Это означает, что ее стоимость и ценность могут зависеть от того, как она распространяется и используется в различных контекстах.

Информация, рассматриваемая как экономический ресурс, имеет множество характеристик, поддающихся анализу через призму системной методологии. А.А. Стрельцов идентифицирует набор таких характеристик, который он классифицирует на две основные группы: содержательные и потребительские свойства[100]. Эти категории позволяют более точно описать характеристики информации как ресурса, который влияет на экономику и общественные процессы.

С формальной точки зрения, информационная система представляет собой совокупность компонентов, которые взаимосвязаны и обусловлены техническими и технологическими особенностями. Согласно Н.Н. Ковалевой, составляющими информационных систем могут являться разнообразные совместимые компоненты, включая техническое оборудование, программное обеспечение и прочие элементы, которые интегрируются для осуществления различных типов информационных процессов[101].

Информационные технологии играют ключевую роль в структуре информационных систем и описаны в Законе об информации[102]. Они охватывают различные процедуры и методологии для поиска, сбора, архивирования, обработки, представления и распространения данных, а также методы реализации этих процессов.

В литературе, посвященной правовым наукам, информационные технологии анализируются через призму трех элементов: объектов, действий и технологических решений[103]. Правовое управление в сфере информационных технологий делится на две ключевые фазы: нормативное урегулирование создания этих технологий и правовое регулирование процесса их применения в дальнейшем.

---

[99] Там же.

[100] Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. … д-ра юрид. наук: 05.13.19. М., 2004. С. 33.

[101] См. Ковалева Н.Н. Информационное право России: учебное пособие. – М.: Дашков и К, 2007. 360 с.

[102] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

[103] Бачило И.Л. Информационное право: Учебник. – М. Издательство Юрайт; 2011. С. 243-244.

Создание и эксплуатация информационных систем, как правило, находятся под правовым воздействием, что связано с необходимостью обеспечения безопасности, защиты данных и соблюдения соответствующих стандартов. Правовое регулирование этих процессов можно рассматривать как важную составляющую производственного сектора экономики, а также как способ стимулирования экономического и социального развития.

Одним из ключевых элементов информационных систем является анализ жизненного цикла информации. Данный цикл состоит из ряда последовательных фаз, на протяжении которых происходит изменение стоимости и релевантности информации. Эта последовательность этапов отображает эволюцию значимости информации со временем и подчеркивает важность обеспечения надлежащего уровня защиты данных на каждом этапе. Уровень безопасности должен соответствовать значению данных, содержащихся в системе, что выделяет необходимость защищать информацию на всех стадиях ее жизненного пути.

Смысловое содержание, формируемое информацией внутри информационной системы, можно охарактеризовать как ее семантическое ядро, обладающее высокой интеллектуальной насыщенностью. Семантическая составляющая охватывает не только совокупность хранимых данных, но также охватывает прикладные решения для вычислительных систем и процедуры, регламентирующие их использование для обработки сведений. Анализировать уровень семантической насыщенности информации возможно исходя из различных критериев, что становится особенно актуальным как при проектировании и эксплуатации информационных систем, так и в процессе формирования нормативно-правовой базы этой сферы.

Для обеспечения сохранности смысла и актуальности сведений, составляющих информационную систему, необходимо организовать корректную обработку данных. Только при условии внедрения алгоритмических механизмов, которые поддерживают постоянное обновление и надежность информации на всем протяжении ее функционирования внутри системы, можно избежать риска частичной либо полной утраты значимых элементов.

Проблематика эксплуатации информационных систем часто коренится в их избыточности. На ранних этапах работы с информационными системами применение разнообразных решений, исполняющих похожие функции, может казаться приемлемым. Тем не менее, с ростом объемов накопленной пользовательской информации, происходит увеличение числа используемых информационных систем. В определенный момент возникает сложность при внесении корректировок в процедуры управления потоками данных, которые затрагивают многочисленные подразделения и сектора из-за необходимости модификации обширного количества уже функционирующих систем. Это часто бывает затруднительно или требует значительных ресурсов, что ставит перед разработчиками и управляющими информационными системами задачу обеспечения их эффективной интеграции и гибкости для обеспечения оптимальной работы всех компонентов системы[104]. Данное положение лишь обуславливает важность реализации принципа правовой интероперабельности.

Согласно ГОСТ Р ИСО/МЭК 15288-2005 «Информационная технология. Системная инженерия. Процессы жизненного цикла систем»[105], система обладает шестью стадиями жизненного цикла:

– стадия замысла. На данном этапе происходит определение ключевых параметров, оказывающих воздействие на права и долги участников правовых отношений на протяжении всего периода функционирования системы. Также осуществляется разбор необходимых требований и четкое выражение главных задач системы;

– стадия разработки. Здесь осуществляется закрепление особенностей последующих стадий, включая привлечение всех заинтересованных сторон к созданию системы и отражение этих аспектов в соответствующих документах, регулирующих процесс разработки;

---

[104] См.: Жернова В.М. Правовой режим информационных систем: дис. … канд. юрид. наук: 12.00.13. Челябинск, 2017. С. 19-34.

[105] ГОСТ Р ИСО/МЭК 15288-2005 «Информационная технология. Системная инженерия. Процессы жизненного цикла систем» (утв. Приказом Ростехрегулирования от 29.12.2005. № 476-ст). М., Стандартинформ, 2006.

– стадия производства. На этой стадии происходит создание и модификация информационной системы. В процессе могут быть внесены изменения в документацию, а также наделены субъекты правоотношений новыми правами и обязанностями, которые не были предусмотрены на предыдущих этапах;

– стадия применения. Это стадия взаимодействия разработчиков, поставщиков и пользователей информационной системы в процессе ее эксплуатации. Здесь важным является совместная работа всех участников для эффективного функционирования системы;

– стадия поддержки применения. В этой стадии осуществляется техническая поддержка и обслуживание информационной системы для обеспечения ее надежной и бесперебойной работы в процессе эксплуатации;

– стадия прекращения применения и списания. Когда система перестает удовлетворять актуальным требованиям или достигнуты новые технологические и правовые стандарты, наступает стадия ее прекращения применения. На этом этапе система выводится из эксплуатации и списывается.

Взаимоотношения, складывающиеся в процессе использования информационных систем, подпадают под регулирование положениями гражданского законодательства. Процедуры разработки и реализации данных систем обычно закрепляются контрактами на проведение научных исследований, экспериментального конструирования и технологических разработок, в соответствии со статьей 769 ГК РФ. В некоторых случаях, помимо договора на разработку системы, также заключаются договоры возмездного оказания услуг или смешанные договоры, если проект включает в себя не только разработку, но и предоставление дополнительных услуг.

Технологическая и формальная части информационной системы регулируются соответствующими техническими стандартами. Эти стандарты необходимы для обеспечения надежности, безопасности и совместимости всех компонентов системы.

Правовое регулирование эксплуатации информационной системы в условиях развития цифровой экономики должно сочетать нормы гражданского права,

касающиеся оказания услуг и выполнения работ, и нормы информационного права, регулирующими такие процессы, как лицензирование и сертификация[106].

Кроме того, помимо общего правового регулирования единых информационных систем, особое внимание уделяется регулированию отдельных элементов. Аппаратные ресурсы, задействованные в операциях по обработке информации, должны отвечать критериям, заложенным в Федеральном законе № 184-ФЗ от 27. 12. 2002 года, именуемом «О техническом регулировании»[107]. Данный законодательный акт определяет обязательные нормы, направленные на гарантирование безопасности и поддержание высокого качества использования технических устройств и систем.

Этот фундаментальный норматив играет ключевую роль в проектировании и эксплуатации оборудования, так как предписывает строгие параметры, устанавливая тем самым юридические основания для унификации технических решений. Он не только защищает конечных пользователей, ориентируя разработчиков и производителей на создание безопасных и надежных продуктов, но и служит важным элементом в стандартизации отраслей, связанных с информационными технологиями, обеспечивая их совместимость.

Следование указаниям данного Федерального закона позволяет компаниям и организациям подтвердить соответствие их технических средств всем принятым стандартам, что, в свою очередь, устраняет технические барьеры в торговле и повышает доверие потребителей к продуктам информационных технологий, укрепляя их позиции на внутреннем и международном рынках.

Информационные системы как объект информационных правоотношений в ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ рассматриваются как

---

[106] Бачило И.Л. Информационное право. Основы практической информатики: учебное пособие. М., 2001. С. 63.

[107] Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // Российская газета. 31.12.2002. № 245.

«совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств»[108].

Анализ категории «информационная система», с точки зрения используемой в Законе об информации дефиниции, позволяет выделить такие основные аспекты как:

1. Сбор информации. Информационная система предназначена для сбора различных видов информации из разных источников, включая сбор данных от пользователей, автоматический сбор информации из внешних источников или другие способы получения информации.

2. Хранение информации. Информационная система обеспечивает правовые механизмы для сохранения и организации информации, включая использование баз данных, файловых систем или других способов хранения информации.

3. Обработка информации. Информационная система проводит различные операции и процессы для обработки информации, в том числе анализ, фильтрацию, сортировку, агрегацию и другие операции, которые позволяют получить нужные данные или преобразовать их для дальнейшего использования.

4. Передача информации. Информационная система обеспечивает механизмы для передачи информации между различными участниками или компонентами системы, включая передачу данных по сетям связи, обмен сообщениями и другие способы.

5. Предоставление информации. Информационная система обеспечивает доступность данных для пользователей или взаимодействующих системных элементов, включая передачу информации средствами интернет-интерфейсов, программных интерфейсов приложений (API) и иных методик предоставления доступа к информационным ресурсам.

А.С. Короткина указывает на то, что информационные технологии, согласно определению термина «информационная система», входят в состав данных систем. Однако анализ правовых норм позволяет прийти к заключению о более высоком

[108] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

режиме этого понятия у законодателя и сделать вывод о том, что информационная система является комплексом объектов материальной и нематериальной формы, объединенных общим предназначением, и, по своей юридической сущности, напоминает сложный объект или вещь. Этот комплекс может содержать множество защищаемых результатов интеллектуального труда в соответствии со статьями 134, 1240 ГК РФ[109].

Так как рассмотрение информационных систем как совокупности материальных и нематериальных объектов создает значительные сложности в правоприменительной практике в части отнесения тех или иных сложных объектов прав к данной категории, то представляется целесообразным выделение категории «технические средства» в качестве самостоятельной категории объектов информационной системы в Федеральном законе № 149-ФЗ[110]. Предложение предполагает распространение на данную категорию режима вещных прав. Реализация этого предложения потребует изменений не только в понятийном аппарате, но и в положениях, касающихся функций оператора информационных систем, а также связанных с ними прав, обязанностей и ответственности.

Технические средства включают в себя аппаратное и программное обеспечение, которые используются для функционирования информационной системы. В сфере информационных систем и компьютерных технологий ключевое значение имеет концепция «программного обеспечения для ЭВМ». В рамках ГК РФ (ст. 1261) этот термин определяется как совокупность запрограммированных инструкций и данных, разработанных с целью выполнения задач на компьютерах или других устройствах, которые производят вычисления.

В рамках данного определения под программным обеспечением понимается не только код программы, но также вспомогательные материалы, появившиеся в ходе ее создания, и визуальные или звуковые данные, производимые в ходе ее функционирования.

---

[109] Короткина А.С. Информационные системы как объект права // Закон и право. 2022. № 5. С. 43-50.

[110] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

Данное понятие распространяется не только на программные компоненты, но и на оформленные в определенный формат сведения, способные стать базой данных. Подобная база данных представляет собой организованную коллекцию информации, которая также имеет право на законную охрану. Авторские права обеспечивают защиту и программного обеспечения для ЭВМ и баз данных, что позволяет сохранять личные и имущественные права их создателей.

Интересно отметить, что авторские права на программные продукты и базы данных существенно отличаются по своему содержанию от права собственности на материальные носители, в составе которых может храниться информация, например, на электронные диски или иные устройства записи. Владение физическим объектом, осуществляющим хранение информации, не означает автоматического приобретения правомочий в отношении размещенного на нем программного обеспечения или базы данных. Соответственно, собственник носителя информации не становится обладателем исключительных прав на программные продукты или информационные ресурсы, которые на нем размещены[111].

Частично базы данных регулируются положениями Федерального закона «О связи» (ст. 53)[112].

Автору программы для ЭВМ или базы данных принадлежат как личные неимущественные, так и имущественные права. Личные неимущественные права включают право на признание авторства, право на защиту репутации автора, в то время как имущественные права позволяют автору извлекать доход от использования произведения, включая право на передачу этих прав другим лицам.

Также объектом информационных правоотношений является информационный ресурс.

Наиболее широко в публикациях по тематике информационных ресурсов представлено определение Ю.П. Шумилова «информационный ресурс – это информация, созданная и (или) обнаруженная, зарегистрированная, оцененная, с

---

[111] Гражданский кодекс Российской Федерации (часть четвертая): Федеральный закон № 230-ФЗ от 18.12.2006 // Российская газета. 22.12.2006. № 289.

[112] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Российская газета. 10.07.2003. № 135.

определенными (заданными) законами деградации и обновления»[113]. Это определение информационного ресурса подчеркивает его режим как ценного актива, требующего управления и поддержки, с учетом процессов создания, обнаружения, регистрации, оценки и обновления информации.

В действующем информационном законодательстве отсутствует дефиниция категории «информационный ресурс», однако этот термин используется в ряде действующих нормативных правовых актов (например, ст. 18 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»[114]).

Отсутствие дефиниции категории «информационный ресурс» в законодательстве может означать, что понимание этого термина оставлено на усмотрение и интерпретацию судебной практики и специалистов, в соответствующих областях. Однако использование термина «информационный ресурс» в нормативных правовых актах указывает на его значимость и применимость в различных сферах.

Следует отметить необходимость рассмотрения специфики концепта «информационный ресурс» на основе анализа его правовой природы и построения понятийного ряда, где базовой категорией является понятие «информация». Существующие представления об информационном ресурсе не всегда полностью охватывают его правовое содержание и не всегда коррелируют с базисными понятиями информационного права. Анализ определений информационного ресурса, приведенных в различных источниках, показывает, что в его состав могут включаться как вся информация в целом, так и ее разновидности. Выделять подмножества можно по разным критериям, например, классам информации или видам документов, которые могут отличаться по способу фиксации на различных носителях и/или возможности обработки с использованием технических средств. Таким образом, наблюдается определенная «размытость» в содержании используемых в настоящее время определений «информационного ресурса»,

---

[113] Шумилов Ю.П. Моделирование информационных ресурсов // Информационные ресурсы России. 2001. № 6. С. 8-9.

[114] Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // Собрание законодательства Российской Федерации. 31.12.2012. № 53 (часть 1). С. 7598.

основанных на концепте «информация», что указывает на необходимость более четкого определения и уточнения содержания данного термина в рамках информационного права.

Информационные услуги являются еще одним объектов информационных правоотношений, которые активно используются в цифровой экономике.

Информационная услуга является правовым явлением, обладающим специфическими характеристиками, связанными с особыми свойствами информации.

Во-первых, информационная услуга обладает целевой направленностью, которая определяется заданием заказчика, соответственно, заказчик активизирует свои информационные потребности путем формулировки информационного запроса или информационного оповещения. Это означает, что информационная услуга ориентирована на удовлетворение конкретных информационных потребностей заказчика.

Во-вторых, действия или деятельность, выполняемые в рамках информационной услуги, включают поиск, сбор, хранение, переработку, систематизацию, распространение и предоставление информации. Информационная услуга включает в себя целый комплекс операций, связанных с обработкой и передачей информации, чтобы удовлетворить информационные потребности заказчика.

В-третьих, процесс оказания информационной услуги фиксируется в нематериальном результате или эффекте самой услуги, то есть информационная услуга не создает материального продукта, а предоставляет информацию, которая может иметь важное значение для заказчика. Результатом информационной услуги является получение и использование информации, которая может помочь в принятии решений, решении проблем или достижении определенных целей.

Информационная услуга обладает особыми свойствами, которые характерны и для дефиниции «информация». Так, информационная услуга, подобно информации, не может быть отчуждена в физическом смысле, не имеет материального носителя и не может быть передана или продана в традиционном

смысле. Вместо этого, информационная услуга представляет собой действия или деятельность, связанную с обработкой и предоставлением информации. Кроме того, информационная услуга может быть предоставлена в различных формах и форматах, таких как текстовые документы, аудио- и видеозаписи, электронные сообщения и другие, не зависит от конкретной формы предоставления, а важна ее содержательная информация. Информационная услуга может быть выделена и отделена от других услуг или деятельностей, так как представляет собой определенный объем информации, который может быть предоставлен отдельно от других услуг или в контексте своей собственной организационной формы. Информационная услуга может быть многократно воспроизведена и предоставлена различным клиентам или пользователям, то есть может быть распространена в большом объеме и использоваться многими людьми одновременно. Также информационная услуга может быть организована и предоставлена в соответствии с определенными процедурами и системами, а также должна быть релевантной и соответствовать целям и запросам заказчика.

Информационная услуга охватывает совокупность процедур и операций, связанных с отбором, накоплением, обработкой, классификацией, передачей и распространением определенного массива данных согласно задачам и требованиям, сформулированным клиентом. Для такого рода услуг характерны особенности, присущие самой информации: невозможность отчуждения, содержательная полнота, способность к отделению от других объектов, многократное воспроизведение, наличие структурированной формы организации и соответствие актуальным запросам пользователя.

Можно предположить, что информационные услуги и консультационные услуги, можно объединить в единую категорию услуг информационного характера[115].

[115] Рустамов П.А. Договор по оказанию информационных услуг: понятие и свойства // Евразийская адвокатура. 2020. № 2 (45). С. 107-109.

Также достаточно интересным нам представляется объект гражданских прав – цифровые права. Авторы постатейного комментария к ГК РФ[116] (ч. 2), следуя буквальному толкованию ст. 128 и 141.1 ГК РФ, считают цифровые права отдельным видом имущественных прав, объектом которых являются обязательственные и иные права[117]. Приведенная категория вызывает определенные возражения[118].

Концепция цифровых прав, охватывающая обязательственные и другие юридически значимые права, упомянутых в списке, представленном в Федеральном законе № 259-ФЗ от 02.08.2019 года (далее — Закон № 259), представляет собой новое направление в правовом регулировании[119]. Они формируют отдельный класс прав, для которых характерно особое закрепление в цифровом формате и зависят от системы приобретения. Тем не менее ГК РФ в статье 141.1 оставляет в тени конкретное содержание этой категории, акцентируя внимание лишь на взаимосвязи с цифровой платформой, на которой эти права реализуются и подтверждаются.

Цифровые права призваны адаптироваться к постоянно развивающемуся цифровому ландшафту, в котором транзакции и взаимодействия осуществляются в виртуальной среде. Важное правовое положение этих прав заключается в том, что они дополняют классическую систему правоотношений, предоставляя такие же степени защиты и гарантии в цифровом пространстве. Процесс их приобретения часто связан с блокчейн-технологиями и уникальными методами верификации, повышающими степени их надежности и безопасности.

Таким образом, хотя основная концепция и виды цифровых прав определены в Законе № 259-ФЗ, практическая и теоретическая разработка их природы, а также

---

[116] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 24.07.2023) (с изм. и доп., вступ. в силу с 12.09.2023) // Собрание законодательства Российской Федерации. 1996. № 5. С. 410.

[117] Гришаев С.П., Свит Ю.П., Богачева Т.В. Постатейный комментарий к Гражданскому кодексу РФ [Электронный ресурс] // Режим доступа: СПС «КонсультантПлюс». (дата обращения: 25.07.2025).

[118] Суханов Е.А. О гражданско-правовой природе «цифрового имущества» // Вестник гражданского права. 2021. № 6. С. 15.; Михеева И.Е. Отдельные правовые особенности залога цифровых прав // Право и экономика. 2022. № 10. С. 18.; Чурилов А.Ю. Перспективы цифровизации товарораспорядительных документов // Юрист. 2021. № 2. С. 10-11.

[119] Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

способы их правовой защиты продолжают оставаться актуальной и весьма дискуссионной темой в современной юридической науке и практике. Это требует от специалистов в области права четкого понимания технологических аспектов цифровых прав, а также умения интегрировать традиционные правовые подходы с новыми цифровыми реалиями.

Закон № 259 написан, по сути, с уклоном в техническую часть. Отсылка к ст. 8 Закона № 259 лишь сужает понятие цифровых прав: права должны существовать в рамках инвестиционной платформы. Уклон в формулировке норм сделан на право требования, что создает впечатление отсутствия возможности принимать цифровые права как что-то новое, они больше похожи на форму подтверждения существующего права.

В законопроекте № 424632–7, в статье 141.1, цифровые права были определены как совокупность электронных данных (цифровой код или обозначения), содержащих информацию об объекте гражданских прав[120]. Однако данное определение подверглось критике с точки зрения эвентуальности, поскольку код не может быть требованием, а значит, не может рассматриваться как право, что ставит под сомнение его отнесение к категории имущественных прав[121]. В частности, В.А. Вайпан подчеркнул необходимость признания в гражданском обороте такого нового элемента как виртуальный объект, который имеет более широкое определение по сравнению с простыми файлами или данными и правами[122]. Закон № 259 утвердил толкование цифровых прав в более узком смысле, определяя их как права требования. Однако такой подход усложняет их включение в гражданский оборот, поскольку ограничивает их применение только к определенным ситуациям, что делает их менее универсальными в правовом контексте.

---

[120] Проект Федерального закона № 424632-7 «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 26.03.2018). URL: file:///Users/mac/Downloads/424632-726032018424632-7.pdf (дата обращения: 05.07.2025).

[121] Вайпан В.А. Право и цифровая экономика // Современные информационные технологии и право: монография / А.С. Ворожевич [и др.]; отв. ред. Е.Б. Лаутс; Моск. гос. ун-т им. М.В. Ломоносова, Юрид. ф-т. М.: Статут, 2019. С. 11-31.

[122] Там же.

Л.А. Новоселова определяет виртуальный актив как особый вид платежного средства или как форму закрепления обязательственных прав[123], что находит поддержку в позиции США, где виртуальные активы рассматриваются как эквивалент ценных бумаг[124]. С.А. Карелина, в свою очередь, указывает на двойственный характер токенов и криптовалют, высказывая предложение о применении «обязательственной теории» для регулирования данных активов, что предполагает их рассмотрение как элементов обязательственного оборота, с соответствующими правами и обязанностями сторон[125].

Необходимо отметить важность четкого определения разновидностей активов, понятие которых получило широкое признание на международном уровне, особенно в рамках работы организаций, таких как Группа по разработке финансовых мер борьбы с отмыванием денег (ФАТФ). Отчет ФАТФ, озвученный 04.07.2019 года, затрагивал нормативное урегулирование оборота виртуальных активов и деятельности сервисных провайдеров данной сферы, включая детальную классификацию последних[126].

Согласно этому отчету, виртуальные активы определяются как значения стоимости, которые можно передавать и обменивать цифровым путем. Кроме того, такие активы могут применяться для инвестирования или в качестве метода осуществления платежей. Чрезвычайно важно подчеркнуть, что виртуальные активы исключают электронные варианты фиатных средств, ценных бумаг или другие финансовые инструменты, регулирование которых подпадает под другие законодательные регламенты ФАТФ.

Финансовая деятельность по отношению к «цифровому финансовому активу» охватывает широкий спектр секторов, связанных с цифровыми финансовыми услугами, в соответствии с трактовкой ФАТФ. В рамках данного

---

[123] Новоселова Л. «Токенизация» объектов гражданского права // Хозяйство и право. 2017. № 12. С. 29-44.

[124] SEC, Report of Investigation under 21 (a) of the Securities Exchange Act of 1934: The DAO, Release № 81207, and Investor Bulletin: Initial Coin Offerings, 25 July 2017.

[125] Карелина С.А., Фролов И.В. Правовой режим криптовалюты и институт несостоятельности (банкротства): проблемы правовой регламентации // Право и цифровая экономика. № 4 (06). 2019. С. 14-18.

[126] Отчет по применению риск-ориентированного подхода. Виртуальные активы и провайдеры услуг виртуальных активов. [Электронный ресурс] URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/MUMCFM-FATF-Guidance-RBA-VA-VASPs.pdf.coredownload.inline.pdf (дата обращения: 02.03.2025).

определения учитываются такие активы, которые могут быть применены для проведения цифровых финансовых транзакций, включая цифровые деньги, различные токены и прочие цифровые инструменты финансирования. Это расширяет объем регулирующих мероприятий в сфере цифровых финансов.

Некоторые ученые говорят об отсутствии специфики в данных правоотношениях, цифровые права выступают как форма субъективных прав[127].

Если мы говорим о встраивании цифровых прав в систему известных объектов, то разумнее всего соотнести их с бездокументарными ценными бумагами, в силу схожести механизма ведения учета.

Различия проявляются в том, что бездокументарные ценные бумаги предполагают наличие контролирующего субъекта, что идет в разрез с механизмом учета цифровых прав[128]. Но можно предположить, что информационная система, в рамках которой существует объект, может выступать как квазисубъект.

Исследователи критикуют использование термина «цифровые права», аргументируя это тем, что на деле это лишь замена наименования для «токена». Никаких реальных прав новая категория на практике не предоставляет, но используется исключительно для бухгалтерского учета и не имеет никаких особых отличительных черт, которые бы выделяли ее среди уже известных юридических объектов[129].

Существует и другой подход, который признает за цифровыми правами особый режим. Согласно нему, понятие цифровых прав обширнее, чем в российском правопорядке, в него входят виртуальное имущество, а в виртуальное имущество входят электронные средства платежа, аккаунты и другое[130].

---

[127] Рожкова М.А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым [Электронный ресурс] // Закон.ру. 2018. 13 июня. // URL: https://zakon.ru/blog/2018/06/13/cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym (дата обращения 26.10.2024).

[128] Новоселова Л., Габов А., Савельев А. и др. Цифровые права как новый объект гражданского права // Закон. 2019. № 5. С. 31-54.

[129] Там же.

[130] Яценко Т.С. Наследование цифровых прав // Наследственное право. 2019. № 2. С. 11-14.; Постановление Девятого арбитражного апелляционного суда от 15.05.2018 г. № 09АП-16416/2018 по делу А40-124668/2017 // СПС «КонсультантПлюс».

Стоит обратить внимание на то, что определение в ГК РФ формирует предпосылки к оценки цифровых прав как узкого понимания цифровых прав, хотя, в то же время, цифровые права поименовываются как самостоятельный объект гражданских прав[131].

Объектами «виртуального мира» могут выступать не только «цифровые права», но любые объекты, существование которых невозможно в реальном мире. Например, аккаунты, трофеи в видеоиграх, игровое оружие, криптовалюта, VR-объекты и многое другие, все это можно включить в категорию «виртуальное имущество».

К виртуальному имуществу можно отнести объекты, существование которых ограничено виртуальным пространством[132]. К отличительным чертам можно отнести: экономическую ценность, существование только в цифровом формате, открытый объектный состав.

Мнения относительно режима виртуального имущества в юридической сфере значительно различаются. Это обусловлено наличием нескольких подходов к его квалификации. Рассматривать явление виртуального имущества возможно, по крайней мере, в четырех ракурсах:

1. Отсутствие специализированного правового регулирования, что означает некую правовую изолированность в этой области.

2. Применение принципов права собственности аналогично тому, как это принято для физических объектов.

3. Использование лицензионных соглашений, которые регулируют взаимоотношения между правообладателем виртуального имущества и его пользователями.

4. Привлечение положений о «другом» имуществе, что предполагает использование общих норм имущественного права для виртуальных активов, не подпадающих под классическое понимание вещественных прав.

---

[131] Гузнов А., Михеева Л., Новоселова Л. и др. Цифровые активы в системе объектов гражданских прав // Закон. 2018. № 5. С. 16-30.

[132] Богданова Е.Е. Проблемы применения смарт-контрактов в сделках с виртуальным имуществом // Lex russica. 2019. № 7. С. 108-118.

Разнообразие этих точек зрения свидетельствует о сложности задачи интеграции виртуального имущества в существующую правовую систему и необходимости разработки универсальных механизмов его регулирования, учитывающих уникальные особенности цифровых активов[133].

На сегодняшний день даже новые объекты, такие как цифровые активы, в основном регулируются через призму интеллектуальной собственности, часто по аналогии с традиционными объектами. Этот подход оказывает значительное влияние на функционирование цифрового оборота, ограничивая его гибкость и адаптивность к современным условиям.

Одним из наиболее распространенных подходов является признание за виртуальными объектами режима объектов интеллектуальных прав, что предполагает включение таких объектов в структуру элементов, охраняемых исключительными правами[134]. Однако важно отметить, что нематериальные объекты, по своей природе, не являются оборотоспособными, в полном смысле этого слова.

Прогрессивное движение рыночной экосистемы цифровых активов укрепляется за счет предоставления эксклюзивных прав на данные объекты. Это правовое устройство служит гарантом интересов для авторов и разработчиков, воздавая им заслуженное признание и финансовую выгоду. Однако, параллельно, такая система прав может налагать определенные ограничения на оборот этих же цифровых благ, потенциально затрудняя свободное использование и распространение в рамках рынка. Согласно А.С. Ворожевичу этот дуализм оказывает значительное воздействие на баланс между стимулированием инновационной деятельности и обеспечением более широкой доступности цифровых активов для пользователей и потребителей[135].

---

[133] Савельев А.И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127-150.

[134] Архипов В.В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9. С. 69-90.

[135] Ворожевич А.С. Исключительные права в цифровой сфере: объекты, границы, пределы осуществления (комментарий законодательства) // В кн.: Современные информационные технологии и право: монография / А.С. Ворожевич, Е.В. Зайченко, Е.Е. Кирсанова и др.; отв. ред. Е.Б. Лаутс; Моск. гос. ун-т имени М.В. Ломоносова, Юрид. ф-т. – Москва: Статут, 2019. – 288 с. – (Труды Юридического факультета: кн. 15). (в соавт.) С. 208-233.

Данный подход можно подвергнуть критике с нескольких сторон. Ограничения, установленные нормами интеллектуальной собственности в отношении цифровых объектов, зачастую вступают в противоречие с задачами рационального и динамичного оборота, поскольку не всегда способствуют облегчению и оптимизации процессов обращения цифровых активов. Подобное регулирование зачастую не соответствует интересам эффективного гражданского оборота и не гарантирует защиту имущественных прав участников, важных для поддержания достоверности и рыночной стоимости объектов на соответствующих рынках.

К тому же, применение исключительно прав интеллектуальной собственности в качестве регуляторного инструмента не обеспечивает полную защиту и не выявляет все потенциальные стороны ценности и преимуществ объекта[136]. Проблематика защиты созданных цифровых работ также актуальна: даже если установлены авторские права на цифровую копию, она не может считаться адекватным объектом в контексте коммерческой деятельности при исключительном использовании методов интеллектуальной собственности. В этом случае, если мы ограничиваемся пониманием виртуальных объектов исключительно через призму интеллектуальной собственности, мы рискуем потерять возможность легального регулирования исходных объектов, что затрудняет их использование в реальной экономике и снижает их потенциал в цифровом обороте. Если мы используем идею о виртуальных объектах только в призме права интеллектуальной собственности, то исходный объект пропадает из страты легального регулирования. Если в реальном мире, созданный предмет (материализованный) охраняется статьей 218 ГК РФ, то в цифровой форме титула собственности не появляется, в силу нематериального носителя результата интеллектуальной деятельности, первичный исходный файл не может быть защищен.

[136] Erlank, W. Introduction to Virtual Property: Lex Virtualis IPSA Loquitur (December 30, 2015). Potchefstroom Electronic Law Journal. Vol. 18. № 7, 2015. [Электронный ресурс]. URL: https://ssrn.com/abstract=2753716.

Анализируя изменения, происходящие в гражданском (цифровом) обороте прав на результаты интеллектуального труда, следует выделить две ключевые составляющие: во-первых, требуется установить, какие правовые режимы применимы к квазиматериальному содержанию; во-вторых, необходимо раскрыть особенности реализации и структуры исключительных прав. Только всестороннее исследование этих аспектов позволяет глубже понять механизмы функционирования и специфику цифрового оборота интеллектуальных объектов.

Информационное общество породило абсолютно новые категории – «цифровые права»[137], «цифровые активы»[138] и «цифровое имущество»[139]. Из перечисленных объектов, нормативное закрепление нашли только цифровые права. Изучив разные точки зрения на данную страту, можно сформулировать черты, свойственные цифровым активам: бинарная форма бытия и обладание ценностью. Помимо наиболее часто ассоциируемых объектов в категории цифровые активы (например, криптовалюта, токены), кажется логичным отнесения к ним больших данных, игрового имущества, аккаунтов и прочего.

В структуре объектов информационно-правового обеспечения цифровой экономики можно отдельно выделить токены, регулирование которых до сих пор не сформулировано. Категория токен имеет многополярное явление. Сначала под токеном понимался монетовидный жетон, например, жетон для слот-машин. Далее под ним понимался электронный ключ безопасности, аппарат для идентификации, в настоящий момент времени под ним именуется разновидность цифрового финансового актива, выпускающийся юридическим лицом или индивидуальным предпринимателем для фондирования и отраженным в реестре операций[140].

---

[137] Эрделевский А.М. О цифровых правах // СПС КонсультантПлюс. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=122169#w4c95nUDLwaxxctW (дата обращения 02.03.2025).

[138] Санникова Л.В., Харитонова Ю.С. Проблемы формирования правовых режимов новых цифровых объектов оборота // Предпринимательское право. Приложение «Право и бизнес». 2019. № 1. С. 37-39.

[139] Егорова М.А., Ефимова Л.Г. Понятие и особенности правового регулирования криптовалют // Предпринимательское право. 2019. № 3. С. 14-16.

[140] Пояснительная записка к проекту федерального закона № 419059-7 «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации». URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения 07.12.2024).

Учитывая то обстоятельство, что рамки диссертационного исследования ограничены, а проблематика исследования посвящена более общим категориям, представляется целесообразным классифицировать токены по группам. Можно выделить четыре группы обсуждаемой категории:

1. Платежные токены – предназначены для использования в качестве платежного инструмента или в качестве средства перевода денежных средств или ценностей;

2. Утилитарные токены – используются для доступа к инфраструктуре (например, приложению), созданной с использованием технологии блокчейн;

3. Токены активов (например, токенизированные акции);

4. Гибридные модели токенов – характеризуются сочетанием свойств ценных бумаг и платежного инструментария[141].

Анализ ряда положений позволяет говорить о том, что рассматривать токены можно с нескольких позиций – как цифровое отражение активов, элемент учета в реестре, хранившая информацию о ценности объекта и правах на него, финансовый инструмент, цифровой код.

Отдельный интерес в рамках темы токенизации правоотношений представляют невзаимозаменяемые токены (NFT). Они выражают конкретный объект в цифровой форме с его характерными чертами. В качестве NFT можно увидеть:

1. Цифровой слепок объекта (картины, художественного произведения).

2. Первообразный нематериальный объект (подобные токены не дублируют объект, а включают в себя. Таким образом, первоначальная ценность формируется по отношению к самому токену).

При анализе действующее законодательство сложно ответить на вопрос, что такое NFT. Однозначно NFT не подпадает под действие Закона о цифровых финансовых активах, NFT не дают права на ценные бумаги, права участия в уставном капитале, право требования передачи ценных бумаг. Также они не

[141] FINMA (16 February 2018). Guidelines for enquiries the regulatory framework for initial coin offerings (ICOs). URL: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

являются цифровой валютой – они не выполняют функцию платежа. Скорее всего, уместнее отнести их к цифровым правам, в соответствии с Гражданским кодексом Российской Федерации.

Также в качестве объектов информационно-правового обеспечения можем выступать технология искусственного интеллекта, в том числе технология беспилотного вождения, данные технологии активно внедряются как государственными компаниями и органами, так и хозяйствующими субъектами.

Например, беспилотное такси от МКПАО Яндекс; роботы доставщики от той же компании. Для регулирования подобных инновация был разработан специализированный нормативных правовой акт – Федеральный законом от 31.07.2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»[142].

Не лишним будет попробовать выстроить систему объектов информационно-правового обеспечения цифровой экономики:

– информационные системы (включая вопросы состояния информационной защищенности);

– технология искусственного интеллекта;

– государственное управление;

– информационная инфраструктура;

– формирование среды для подготовки работников (в качестве примера, может выступать создание Инновационного центра «Сколково»).

– в качестве самостоятельного сформированного объекта информационного правового обеспечения цифровой экономики выступают экспериментальные правовые режимы;

– финансовые отношения (инкорпорация цифровых финансовых активов, цифрового рубля);

[142] Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru), 31.07.2020, ст. 0001202007310024. URL: http://publication.pravo.gov.ru/Document/View/0001202007310024.

– сквозные технологии (включая квантовые, «большие данные»)[143];

– машинное обучение;

– и другие.

Отметим, что в любую цифровую технологию входят направления развития субтехнологий (например, нейротехнологии и искусственный интеллект включают в себя компьютерное зрение, нейроинтерфейс и другое)[144].

Необходимо упомянуть процесс «токенизации» или «алгоритмизации» права (в качестве явной тенденции можно привести пример с трансформацией корпоративных отношений (цифровые права), договорного права (самоисполняющиеся контракты). «Алгоритмизация» права порождает абсолютно новые категории, которые только предстоит вписать в структуру правоотношений.

Названный перечень объект остается открытым в силу стремительного развития современных технологий. Учитывая то обстоятельство, что право вторично, сформулированные объекты являются наиболее явными и требующими изучения.

Экспериментальные правовые режимы (далее — ЭПР) были введены в 2020 году Федеральным законом от 31.07.2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». Экспериментальные режимы могут вводиться в определенных сферах:

– медицине;

– проектировании и производстве транспортных средств;

– сельском хозяйстве;

– финансовом рынке;

– продажах товаров, выполнение работ, оказание услуг дистанционном путем;

– промышленности;

– и ряде других направлений, установленные Правительством РФ.

---

[143] Вайпан В.А. Цифровое право: истоки, понятие и место в правовой системе // Право и экономика. 2024. № 1. [Электронный ресурс]. Режим доступа: СПС «КонсультантПлюс».

[144] Там же.

Под экспериментальным режимом понимается применение специального правового регулирования по отношению к участникам такого режима на определенном промежутке времени.

Основополагающими задачами для экспериментальной правовой системы являются стимулирование появления инновационных форм экономической активности, усиление конкурентоспособности, стимулирование прогресса в научной и социальной среде, а также улучшение управленческого регулирования в соответствии с результатами применения данного режима.

Важной целью также является привлечение инвестиций, которые направлены на форсирование предпринимательских начинаний в области цифровых технологий. Рассматриваемый правовой режим представлен как временная мера, рассчитанная на период, необходимый для внедрения и распространения цифрового новшества, и не превышает трех лет.

Тем не менее, данный срок может быть продлен на один год — до 12 месяцев, в случае, когда Правительство принимает такое решение, основываясь на подаче мотивированного обращения от ведущего органа.

Мониторинг деятельности субъекта ЭПР осуществляет компетентный орган. Правовой режим может быть изменен, приостановлен или прекращен.

Что касается информационной инфраструктуры, то в нее можно включить: образовательные центры, инновационные центры, экспериментальные правовые режимы по соответствующим направления развития.

Формирование новой экономической системы (new normal, новой реальности[145]), в плоскости права появляется система, которая отлична от традиционной, она требует введения в правовую сферу новых способов взаимодействия между хозяйствующими субъектами, формирования нового подхода к антимонопольному регулированию и инфраструктуры.

[145] Медведев Д.А. Новая реальность: Россия и глобальные вызовы // Вопросы экономики. 2015. № 10. С. 5-29.

При рассмотрении сущности цифровой экономики одной из ключевых целей является установление легальных форм структурирования общественных отношений, для этого выделяют реперные точки:

– правовой статус субъектов;

– реализацию правоотношений;

– правовой режим объектов правоотношения;

– сущностное наполнение правоотношений[146].

Также в качестве проблемы можно говорить об отсутствии должной инфраструктуры, которая бы упростила переход в цифровую эру (хотя подобные идеи сформулированы в программных и стратегических документах)[147].

Система цифровой экономики содержит в себе три уровня:

– рынки;

– цифровые платформы;

– стимулирование[148].

Далее можно рассмотреть аккаунты в социальных сетях. Аккаунт выполняет функцию идентификации пользователя в рамках определенной информационной системы, более того, учитывая обстоятельства наполнения аккаунта (создание контента, монетизация его), аккаунт может представлять экономическую ценность, кроме этого, на него можно распространить положения института интеллектуальной собственности.

Если мы попробуем классифицировать аккаунты, то столкнемся с проблемой систематизации, а именно, сложностью выделения критерия систематизации. Одной из возможных классификаций является:

– аккаунты внутри социальных сетей (делятся на профессиональные/коммерческие и личные/для индивидуального использования);

---

[146] Попондопуло В.Ф. Правовые формы цифровых отношений // Юрист. 2019. № 6. С. 29-36.

[147] Постановление Правительства РФ от 02.03.2019 № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 11. Ст. 1119; Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

[148] Кузнецов П.У., Харитонова Ю.С. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 1. С. 154-161.

– аккаунты для осуществления платежей и аккаунты интернет-маркетплейсов;

– профили для геймеров;

– электронные почтовые ящики.

Также Е.Е. Кирсанова выделяет аккаунты без подтверждения личности и подтвержденные аккаунты[149].

Следует отметить, что на сегодняшний день нормативное определение термина «аккаунт» отсутствует, что создает неопределенность в правовом регулировании этой категории. На практике под аккаунтами обычно понимается средство для передачи и (или) распространения информации.

Обсуждается понятие «владелец профиля в социальных сетях», которое порождает дискуссии по поводу адекватности использования термина «владение» в данном контексте. Традиционно, владение ассоциируется с реальным владением физическими объектами, тогда как профили в социальных сетях представляют из себя цифровые сущности, что вызывает споры относительно того, возможно ли применять такую категорию к нематериальным активам. Согласно нормам права, ключевая характеристика, определяющая владельца имущества, заключается в его властном распоряжении им[150].

При этом учетная запись пользователя в сети «Интернет», в отличие от корпоративных активов или недвижимости, составляет информационный ресурс, который зачастую сложно подвести под категорию физической собственности. В силу своей нематериальной природы право собственности на аккаунт в социальной сети не всегда отчетливо определено и подпадает под различные юридические интерпретации. Это существенно комплицирует (усложняет) правовой статус владельца профиля и принципы регулирования его взаимодействия с созданной цифровой средой. Право владеть собственностью является фундаментальной

[149] Кирсанова Е.Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: монография. – М.: Юстинцинформ, 2022. С. 101.

[150] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 14.01.2020 № 225-АПУ19-4. (текст опубликован не был) // СПС «КонсультантПлюс».

привилегией, однако ее применение к цифровым аккаунтам требует уточнения и, возможно, разработки специализированных нормативных актов.

Именно такие недостатки в правовом обеспечении приводят к необходимости более глубоких исследований в этой области, что, в свою очередь, может способствовать развитию юридических доктрин и обновлению регулирования в эпоху цифровизации. Кроме того, эволюция правового понимания имущественных отношений в виртуальном пространстве открывает перед законодателем новые перспективы в адаптации существующих законов к меняющимся реалиям цифрового мира.

Под имуществом подразумевается не только физические объекты, но и интеллектуальные активы, включая права собственности и цифровые права. Это позволяет рассматривать учетные записи как элементы имущественного портфеля, что находит подтверждение в судебной практике[151].

Говоря о природе аккаунтов, можно прийти к выводу, что они формируют уникальную категорию «псевдоимущества», которое не вписывается в классические рамки объектов собственности, однако оно может быть причислено к предметам гражданского права.

Такой подход допускает возможность рассмотрения аккаунтов как независимых предметов гражданско-правовых отношений или же как компонента имущественного комплекса, что находит отражение в определенных решениях судебной практики. Это открывает новые перспективы для правового регулирования цифровых активов и их признания частью имущественных прав в рамках современного цифрового оборот[152].

Аккаунт можно рассматривать как:

– нематериальный объект;
– информационную площадку;
– самостоятельный оборотоспособный объект.

---

[151] Там же.

[152] Постановление Тринадцатого арбитражного апелляционного суда от 17.01.2018 № 13АП-30540/2017 по делу № А21-6695/2017 // СПС «Консультант Плюс».

Можно провести параллель между аккаунтом пользователя и структурами, подобными базе данных, шифровке данных пользователем на серверах, принадлежащих владельцу социальных сетей, а также условиями, прописанными в договорных отношениях с управляющими социальной сетью.

Каждый из подходов несет в себе определенные несовершенства и не обеспечивает комплексного решения по вопросу юридического положения пользовательских аккаунтов. Это приводит к необходимости дальнейшего изучения и определения природы аккаунтов в правовом поле, учитывая тонкости цифрового владения и узаконивания соответствующих отношений между пользователями и провайдерами услуг социальных сетей[153].

Первоначально следует обратить внимание на положения статьи 1260 ГК РФ, которая характеризует базу данных как совокупность независимых элементов (включая тексты, данные, законодательные акты, судебные постановления и аналогичные материалы), организованных таким образом, что их можно отыскать и обработать с применением компьютерной технологии. Для предоставления базе данных правовой защиты необходимо выполнение условий статьи 1334 ГК РФ. Эта статья требует значительных инвестиций ресурсов – финансовых, материальных или организационных – или включения в базу не менее десяти тысяч отдельных единиц информации. В контексте учетной записи эти параметры могут быть неприменимыми из-за того, что учетная запись зачастую не является структурированным набором данных подобным базе данных и, следовательно, может не подпадать под одинаковую правовую защиту.

Можно понимать аккаунт как набор данных, хранящийся на сервере. Однако такой взгляд не дает исчерпывающего ответа на вопрос о юридическом режиме этих данных. Так, связь аккаунта с сервером не влечет за собой неизменную правовую классификацию, поскольку информация в аккаунте динамична и подвержена изменениям, обусловленным пользовательской активностью на платформе.

---

[153] Панарина М.М. Наследование аккаунта в социальных сетях и вопросы цифрового наследования: правовое исследование // Наследственное право. 2018. № 3. С. 29-30.

Можно предположить о том, что устанавливается связь аккаунта с набором прав и обязанностей, исходящих из пользовательского соглашения с провайдером социальной сети. В этой перспективе важным является взаимодействие между владельцем аккаунта и оператором платформы: последний задает правила взаимодействия в сети, тогда как пользователь принимает эти правила, соглашаясь на них и, соответственно, руководствуясь ими при размещении и обработке своего контента.

Л.Ю. Михеева отмечает, что размещение материала в социальной сети не тождественно согласию на использование этого материала, его использование должно оцениваться судебными инстанциями в каждом конкретном случае. Это подчеркивает важность индивидуального подхода к правовым последствиям размещения контента и использования аккаунтов, что делает правовое регулирование аккаунтов сложным и многогранным процессом[154].

Третий подход к правовой природе аккаунта представляется жизнеспособным при соблюдении двух ключевых элементов. Во-первых, аккаунт существует не только в социальной сети, но и в другой информационной системе, такой, как личный кабинет в онлайн-сервисе. Во-вторых, должен быть урегулирован вопрос перехода прав на аккаунт, например, через уступку прав. Это позволяет рассматривать аккаунт как объект, который может быть передан или изменен в рамках гражданского оборота, что подчеркивает его ценность в юридическом контексте[155].

Аккаунты можно разделить на две группы:

– аккаунты, предоставляющие право доступа в информационную систему, но не обладающие самостоятельной ценностью. Эти аккаунты предоставляют возможность получения чего-то в будущем (например, личный кабинет онлайн-магазина), но сами по себе не являются объектами с явной экономической ценностью;

---

[154] Михеева Л.Ю. Объекты гражданских прав: правовые позиции, содержащиеся в Постановлении Пленума Верховного Суда Российской Федерации «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» // Судья. 2015. № 10. С. 18.

[155] Панарина М.М. Наследование аккаунта в социальных сетях и вопросы цифрового наследования: правовое исследование // Наследственное право. 2018. № 3. С. 29-30.

– аккаунты с экономической ценностью, такие как страницы в социальных сетях с большим количеством подписчиков и рекламными контрактами, которые могут выступать в качестве независимых объектов оборота. Эти аккаунты могут иметь реальную стоимость, которая определяется их популярностью, а также возможностью использования для коммерческих целей, таких как реклама и продвижение товаров и услуг.

Суды также часто используют категорию аккаунтов в контексте правовых решений, что подтверждается практикой рассмотрения дел, в которых акцент делается на эвентуальность оформления договоров купли-продажи аккаунтов. Суды не исключают возможности признания аккаунта самостоятельным объектом гражданских правоотношений, что открывает новые горизонты для правового регулирования этого вида активов[156].

Следственно, аккаунт в сети «Интернет» представляет собой энтитет, вокруг которого неизбежно возникает необходимость специализированного нормативного регулирования. Однако, основываясь на конкретных свойствах и функциях аккаунта, его также можно отнести к более обширному термину, такому как «цифровое имущество» или «цифровой актив», что подразумевает включение в рамки уже сформировавшихся категорий правового поля.

Развивающимся элементом цифровой экономики стали цифровые платформы. На сегодняшний день высказываются идеи о выделении нового направления научно-правовой деятельности – формировании платформенного права[157].

В современной цифровой экономике онлайн-платформы выступают средствами, обеспечивающими новые пути распространения продукции и оказания различных услуг. С их помощью формируются эффективные форматы взаимодействия между сторонами, например, кредиторами и должниками, тогда

---

[156] Постановление Тринадцатого арбитражного апелляционного суда от 17.01.2018 № 13АП-30540/2017 по делу № А21-6695/2017 // СПС «Консультант Плюс».

[157] Кашкин, С. Ю., Алтухов, А. В., Пожилова, Н. А. Платформенное право как инструмент инновационных инвестиционных платформ (краудфандинг) // Вестник Университета имени О. Е. Кутафина. 2021. № 1 (77). С. 157-166. URL: https://cyberleninka.ru/article/n/platformennoe-pravo-kak-instrument-innovatsionnyh-investitsionnyh-platform-kraudfanding.

как третьим участником процесса становится управляющая платформа организация, выполняющая функцию посредника и регулирующего звена в деловых отношениях[158].

Один из терминов, применяемых относительно цифровых платформ – «marketplace»[159] – демонстрирует экономическую направленность проекта. Существующие площадки можно сгруппировать следующим образом:

– платежные (PayPal);
– информационно-интегрированные (Google, Uber);
– инвестиционные (SoftBank);
– инновационные (Oracle);
– обучающие (Coursera);
– социальные (VK).

Учитывая специфику площадок, в общих случаях они не являются объектами обеспечения цифровой экономики, они ближе к составным частям инфраструктуры, однако существуют обстоятельства, при которых они могут выступать оборотоспособными и быть объектами. Опять же используя аналогию, действующих по отношению к имущественному комплексу, наподобие предприятий. Можно предположить надобность корректировки законодательства, выделить цифровые платформы как новый вид имущественного комплекса. В подтверждение факта выделения новых объектов цифровой экономики можно привести пример с социальными сетями[160]. В соответствии с действующим законодательством социальными сетями можно владеть[161]. Также ФАС России в письме «О разъяснении по вопросу рекламы в информационно-телекоммуникационной сети Интернет» указывает на право на размещение определенного типа информации на сайтах, «владельцем которых является

---

[158] Карцхия А.А. Цифровые технологические (онлайн) платформы: российский и зарубежный опыт регулирования // Гражданское право. 2019. № 3. С. 25-28.

[159] Рынок (Прим. – *перевод Автора*).

[160] Кирсанова Е.Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: монография. – М.: Юстинцинформ, 2022. С. 102-114.

[161] См.: ст. 10.6. Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

учредитель телеканала спортивной направленности», также ФАС России пишет о направлении запросов «владельцам социальных сетей»[162].

Подводя итог, можно прийти к выводу о том, что в период цифровой экономики выделяются два вектора развития отношений: появляются новые объекты в сфере цифровой экономики и трансформируются ранее известные объекты. Некоторые появляющиеся объекты в полной мере не являются новыми, а представляют собой лишь новую форму ранее известного объекта. Особого регулирования заслуживает виртуальное имущество, так как такие объекты лишены, по сути, необходимой защиты[163].

При рассмотрении объектов информационно-правового обеспечения цифровой экономики необходимо упомянуть о технологии искусственного интеллекта. На сегодняшний день технологию искусственного интеллекта, регулируется «Национальной стратегией развития искусственного интеллекта на период до 2030 года»[164]. Стратегия развития содержит два важных термина (в рамках исследования): искусственный интеллект (определяя его как комплекс технологических решений, позволяющих имитировать когнитивные функции человека…) и технологии искусственного интеллекта как технологии, основанные на искусственном интеллекте, что представляется не совсем верным, так как технологии являются отдельными случаями применения искусственного интеллекта, представляется обоснованным в рамках научного дискурса (настоящего исследования) уравнивать данные категории.

В настоящий момент, самый релевантным подходом представляется признание технологии искусственного интеллекта как источника повышенной опасности (далее - ИПО), так как он отвечает реалиям развития технологии и состоянию правовой сферы[165]. В качестве аргументов можно привести следующие:

---

[162] Письмо ФАС России от 25.09.2019 № АК/83509/19 «О разъяснении по вопросу рекламы в информационно-телекоммуникационной сети Интернет». URL: https://fas.gov.ru/documents/ak-83509-19.

[163] Рустамов П.А. Объекты информационно-правового обеспечения цифровой экономики // Евразийская адвокатура. 2024. №. 6 (71). С. 167.

[164] Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента РФ «О развитии искусственного интеллекта в Российской Федерации» от 10.10.2019 № 490) // Собрание законодательства Российской Федерации. 2019 г. № 41. Ст. 5700.

[165] Необходимо сделать оговору, что применение конструкции источника повышенной опасности по отношению к технологии искусственного интеллекта оправдано с точки зрения публично-правового значения, так

– *Автономность и непредсказуемость поведения технологии искусственного интеллекта:* неустранимая неопределенность: современные ИИ-системы (особенно глубокого обучения) работают по принципу «черных ящиков», не всегда представляется возможным предсказать реакцию на входные данные, что создает риски в критических сферах (медицине, транспорте). В рамках описанной концепции отношения будут подпадать под действие ст. 1079 ГК РФ. Российскому подходу об источниках повышенной опасности говорит о том, что у объекта должна присутствовать характеристика, согласно которой нормальное функционирование объекта невозможно без наличия риска причинения вреда. Технология искусственного интеллекта соответствует данному критерию в силу своей алгоритмической природы.
– *Масштаб потенциального вреда:* роботы, управляемые искусственным интеллектом, могут стать причиной травм из-за сбоев ПО. В социально-экономическом плане возможна дестабилизация общества (через генерацию “deepfakes” для манипулирования выборами, распространение дезинформации через социальные сети, автоматизированные кибератаки на инфраструктуру), дискриминация (алгоритм кредитного скоринга воспроизводит скрытые предубеждения).
– *Проблема установления причинно-следственной связи и ответственности:* диффузная виновность (ответственность), при которой вред, нанесенный технологией искусственного интеллекта сложно персонализировать. Кроме того, традиционные нормы деликтного права не учитывают самообучение технологии,

---

как технология искусственного интеллекта носит потенциально высокий риск для общества, прослеживается объектная потребность публичной власти в регулировании данной сферы. Правовая конструкция источника повышенной опасности носит междисциплинарный характер, что подтверждается наличием научных работ в плоскости не только частного права, но и публичного. Например, Зенцова С.А. Источник повышенной опасности и его уголовно-правовое значение: автореф. дис. ... канд. юрид. наук: 12.00.08. Науч.-исслед. ин-т Федерал. службы исполнения наказаний. М., 2006. С. 5.; Жернова В.М. Информационные системы как источник повышенной опасности в условиях цифровизации // Вестник ЮУрГУ. Серия «Право». 2019. № 3. С. 67-71.

нестандартный результат взаимодействия между компонентами системы, непредвиденные последствия при работе в открытой среде.

- *Коллатеральные последствия даже при «корректной» работе:* существует ряд смежных рисков – экологический риск (центры обработки данных потребляют большое количество энергии), в сфере медицины (модели диагностики, обученные на нерепрезентативных данных, пропускают болезни у определенных групп пациентов, например, у этнических меньшинств).
- *Неэффективность превентивных мер контроля:* можно выделить технические ограничения, такие как неопределенность калибровки (методы оценки «уверенности» технологии ненадежны, система часто гиперконфидентна при ошибках) и регуляторное отставание.

Признание технологии искусственного интеллекта источником повышенной опасности оправдано по следующим критериям:

- неустранимость риска при должном использовании;
- необходимость специального режима ответственности.

Данное обстоятельство потребует: страхования ответственности для операторов (владельцев); создание компенсационных фондов; внедрения «черных ящиков» для фиксации решений искусственного интеллекта в реальном времени.

Страховой фонд может выглядеть следующим образом.

Фонд страхования ответственности за вред, причиненный технологией искусственного интеллекта, должен сочетать обязательные взносы операторов, участие государства и механизмы оперативного возмещения. Источником финансирования могут быть обязательные страховые взносы для участников рынка (операторов/разработчиков/владельцев), например, от 0,5 % до 5 % от оборота пропорционально уровню потенциальной угрозы; государственные субсидии (на начальном этапе и при отсутствии происшествий); штрафные санкции; добровольные взносы.

Таблица 1 – Размер взносов для участников рынка

Класс технологии искусственного интеллекта	Ставка взноса	Минимальная страховая сумма
Медицина/транспорт	4 %	1 млрд. руб. на систему
Финансы/энергетика	2,5 %	400 млн. руб.
Рекомендательные	1 %	100 млн. руб.

Для определения величины выплаты необходима классификация рисков.

Механизм выплаты должен сочетать в себе несколько элементов – легкость, ограниченность выплаты и регрессные требования фонда. Упрощенная процедура для пострадавших формируется из наличия доказательной базы (факт вреда и наличие причинной связи с технологией, без доказывания вины) и минимального срока (месяц на выплату). Ограниченность ответственности – на конкретное физическое лицо до 100 млн. руб., при «массовом» ущербе до 400 млн. руб. на инцидент. Также должно присутствовать право у фонда на взыскание суммы с виновных операторов/разработчиков при доказанной халатности. Управление, а также контроль за деятельностью фонда, должно включать наблюдательный совет, в состав которого должны входить представители органов государственной власти (Минцифры России, Роскомнадзора), эксперты в сфере технологии искусственного интеллекта (инженеры, ученые), представители общественности (ассоциации потребителей, юристы). Функции совета представляют собой актуарный аудит, формирование инвестиционной политики, мониторинга «черных ящиков» (доступ к логам решений искусственного интеллекта при расследовании инцидентов).

Модель в России представляется двухэтапная – первый этап: обязательная регистрация технологии искусственного интеллекта в Роскомнадзоре, формирование страхового (компенсаторного) фонда; второй этап – автоматизация выплат (с инкорпорацией алгоритмов смарт-контрактов) и создание центра аудита рисков.

Необходимо выявить плюсы концепции источника повышенной опасности (ИПО), по сравнению с концепцией электронного лица (КЭЛ):

1. *Отсутствие автономии vs. юридическая фикция.* ИПО-подход четко признает, что технология искусственного интеллекта является инструментом, созданным и контролируемым людьми. Риски возникают из-за технической сложности, а не «сознания». КЭЛ-подход наделяет технологию квазисубъектностью, создавая опасную иллюзию автономии. В самом деле технология искусственного интеллекта не обладает (на сегодняшний день) самосознанием или волей, способностью нести ответственность и не может компенсировать ущерб, на данный момент времени.
2. *Гарантированная защита пострадавших.* ИПО-подход вводит строгую (безвиновную) ответственность, в соответствии со ст. 1079 ГК РФ. Пострадавшим необходимо лишь доказать факт вреда и связь с технологией. КЭЛ-подход требует доказывать «вину» технологии, что технически невозможно.
3. *Экономическая эффективность.* ИПО-подход четко распределяет риски (страхование как опасного объекта; фонд возмещения вреда; создает стимулы для бизнеса к инвестициям в безопасность), КЭЛ-подход, в свою очередь, вводит «двойную» бухгалтерию (искусственное «имущество» технологии будет находиться на балансе компании-владельца), предоставляет уход от ответственности (разработчики/владельцы переведут активы на «электронное лицо» с нулевой платежеспособностью).
4. *Совместимость с правовыми системами.* ИПО-подход не требует масштабных изменений в праве, экономит правовую мысль. КЭЛ-подход требует создания новых процессуальных норм, «прав» на неодушевленные объекты, глобальной конвенции о статусе технологии.
5. *Управление рисками ex-ante.* ИПО-подход фокусируется на предупреждении вреда (через обязательную сертификацию технологии, «черные ящики» для фиксации решений, запрет на применение в

критических сферах без страхования). КЭЛ-подход переносит акцент на последствия, а не профилактику.

Таким образом, изучение объектов информационных правоотношений играет важную роль в правовом регулировании цифровой экономики. Оно позволяет определить и разработать соответствующие правовые нормы и механизмы, обеспечивающие защиту прав и интересов участников цифровой экономики, а также способствуют развитию и инновациям в этой сфере. Информационные правоотношения – это общественные отношения, регулируемые правом и включающие в себя носителей информационных прав и обязанностей, связанных с перераспределением информации о лицах, предметах, фактах, событиях, явлениях и процессах в обществе, независимо от формы ее представления. В следующем параграфе Автором будет рассматриваться идея о наделении правоспособностью (ограниченной или полной) технологии искусственного интеллекта, однако как обозначается в работе, на сегодняшний день, это преждевременно, но представляет интерес с научной точки зрения и представленная позиция являет собой потенцию для дальнейшего развития по прошествии времени, особенно учитывая то обстоятельство, что появление «сильного» искусственного интеллекта неминуемо поставит данную задачу.

§ 1.3. Субъекты информационно-правового обеспечения в сфере цифровой экономики

В условиях быстрого развития информационно-телекоммуникационных технологий, появление новых субъектов права и изменение общественных отношений является неотъемлемой реальностью, существенно влияющей на информационно-правовую сферу и систему информационного права. В связи с этим, возникает необходимость разработки общетеоретических концепций, которые бы определили системную организацию субъектов правовой жизни, их функциональные характеристики и взаимосвязи.

Субъектами отношений в сфере информационного права выступают как отдельные физические лица, так и организации различной правовой формы, а также органы государственного и муниципального управления. Все эти участники действуют как в рамках частноправовых, так и публично-правовых механизмов, осуществляя операции с информацией. Принимая участие в таких процессах, граждане и организации получают определенный набор юридических прав и обязанностей, регулирующих обращение с информационными ресурсами — начиная с их сбора и анализа, вплоть до хранения и передачи третьим лицам.

Данные права включают право на доступ к информации, право на неприкосновенность частной жизни и защиту данных, а также право на защиту интеллектуальной собственности. Органы местного самоуправления, такие как муниципальные советы или администрации, являются субъектами информационного права, поскольку они несут ответственность и осуществляют полномочия по управлению и предоставлению доступа к публичной информации в пределах своей юрисдикции, отвечают за обеспечение прозрачности, подотчетности и защиту прав граждан на доступ к информации.

В системе информационного права государственные структуры, среди которых выделяются агентства и надзорные органы, наделены обширными функциями в управлении информационными потоками, формировании и реализации государственной политики в данной сфере. К их задачам относятся контроль за исполнением нормативных предписаний, разработка стратегий по охране публичных интересов, обеспечение национальной безопасности в информационной среде.

Участники информационно-правовых отношений представляют собой не только отдельные лица или организации, но и субъектов, обладающих закрепленными в российском законодательстве правами и обязанностями. В процессах, связанных с доступом к данным, в особенности при обращении с официальными документами или при функционировании средств массовой информации, центральное место занимают те, кто выступает в роли пользователей информации. Им предоставлена законная возможность реализовать

основополагающее право на поиск, получение и использование сведений в соответствии с положениями Конституции.

Примерами таких субъектов являются граждане Российской Федерации, государственные и негосударственные предприятия, муниципальные предприятия, органы государственной власти, муниципальные органы, журналисты, различные виды потребителей рекламы и другие. Владельцы информации также считаются субъектами данных правоотношений.

С.Г. Чубукова подчеркивает значимость разграничения между терминами «субъект информационного права» и «субъект информационного правоотношения». «Субъект информационного права» описывает индивидов или коллективы, участвующие в процессах взаимодействия с информацией и имеющие конкретный набор прав и обязанностей в этой области. Это понятие тесно переплетается с «субъектом информационного правоотношения», указывая на участников, чьи взаимоотношения регулируются информационным правом.

Субъект информационного правоотношения – это субъект, участвующий в конкретном информационном правоотношении, возникающем между двумя или более субъектами информационного права. Информационное правоотношение представляет собой юридическую связь между субъектами, основанную на обмене, использовании или распространении информации. Таким образом, субъект информационного права является более общим понятием, охватывающим всех участников информационных отношений, обладающих правами и обязанностями в сфере информации. В то же время субъект информационного правоотношения – это конкретный участник информационного правоотношения, взаимодействующий с другими субъектами в рамках определенного информационного отношения[166].

Субъекты информационно-правовых отношений могут быть классифицированы на основе различных критериев. В контексте взаимодействия с информацией, к ключевым участникам относятся индивиды и организации,

[166] Чубукова С. Г. Цифровая трансформация системы субъектов информационного права // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12. С. 74-81.

которые занимаются созданием, изменением, передачей, распространением, приемом и использованием информации[167].

Создатели или производители информации являются одним из основных субъектов информационного права. Данная категория субъектов информационных правоотношений создают информацию путем исследований, создания произведений и других форм творчества. Примерами таких субъектов могут быть авторы книг, журналисты, художники, музыканты и другие творческие личности.

Обладатели информации являются субъектами информационных правоотношений, владеющими информацией и контролирующие ее использование и распространение. Это могут быть организации, государственные учреждения или частные лица, обладающие информацией, которая имеет стоимость или стратегическое значение.

Потребители информации также являются важными субъектами информационных правоотношений, получая и используя информацию для различных целей, включая принятие решений или удовлетворение своих информационных потребностей и тому подобное.

В.В. Сафронов акцентирует внимание на том, что если говорить о базовых принципах категоризации участников правовых отношений, то участники информационных правоотношений могут быть классифицированы следующим образом:

– индивидуальные участники, то есть физические лица, которые задействованы в информационной деятельности и обороте информации;

– коллективные участники – юридические лица, независимо от того, к какой форме собственности или каким организационно-правовым формам они принадлежат[168].

Существующие классификации субъектов информационных правоотношений не учитывают то, что в условиях цифровизации, традиционная

---

[167] Лукашевич С.А. Некоторые аспекты гражданско-правового статуса информации // Вопросы российского и международного права. 2021. Т. 11. № 2 А. С. 33-39.

[168] Сафронов В.В. Субъекты информационных правоотношений // Решетневские чтения. 2010. С. 556-557.

система субъектов информационного права претерпевает изменения в результате появления новых субъектов. В связи с этим в рамках данного исследования предлагается следующая классификация субъектов информационных правоотношений, основанная на их правовом статусе, ролях и функциях, которые они выполняют в правовых отношениях. В рамках данной классификации предлагается выделить следующих субъектов информационных правоотношений:

– физические лица, участвующие в информационном процессе;

– юридические лица, участвующие в информационном процессе;

– органы государственной власти, регулирующие информационные процессы;

– квазисубъекты, участвующие в информационном процессе.

В качестве участников информационных правоотношений физические лица могут выступать в различных ролях и выполнять различные функции. Так, к физическим лицам как субъектам информационных правоотношений относятся потребители информации, создатели информации, пользователи информационных систем и лица, осуществляющие защиту прав потребителей информации.

Исследуя сферу цифровой экономики, важно отметить, что субъектами информационных правоотношений могут быть не все лица, а лишь те, которые наделены действующим законодательством определенными правами и обязанностями. В наиболее широком понимании сторонами данных правовых связей выступают физические и юридические лица, публичные образования и институты.

На основании изложенного, в рамках анализа фундаментальных критериев классификации участников правовых отношений, можно выделить две главные категории субъектов информационных правоотношений:

– индивидуальные субъекты – это физические лица, задействованные в процессах информационного обмена и оборота;

– коллективные субъекты – юридические лица, независимо от форм собственности и организационно-правовых форм, которые участвуют в информационном процессе[169].

Цифровизация процессов, происходящих в общественной жизни, занимает все более значимое место, что изменяет как саму природу правоотношений, так и участников этих процессов. Одним из ярких проявлений этого явления является активное внедрение цифровых платформ, которые в значительной степени изменяют субъектный состав информационных правоотношений. На этих платформах происходит не только обмен информацией, но и трансформация ролей участников в цифровой среде, что требует новых подходов в правовом регулировании и классификации субъектов.

Дискуссии по поводу правового регулирования их функционирования со временем не теряют своей актуальности. Д.А. Гаврин выделяет такие темы для обсуждения, как алгоритм и право, проблема безграничности сети, совершение юридически значимых действий[170]. А.А. Белоусов отмечает, что платформы «переформатируют работу финансового рынка в аспекте взаимоотношений продавцов и потребителей финансовых услуг»[171]. И.Ш. Исмаилов обращает внимание на проблему распределения ответственности между платформой и поставщиками финансовых услуг[172].

В Законе об информации основными субъектами в данной сфере являются: оператор информационной системы, обладатель информации и провайдер хостинга. В Федеральном законе от 20. 07. 2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы»[173] (далее — Закон о финансовых платформах) указаны следующие субъекты:

---

[169] Боер В.М., Павельева О.Г. Информационное право: учеб. пособие. Ч. 1 / ГАУП. СПб., 2006. с. 47-48.

[170] Гаврин Д.А. Особенности совершения сделок с использованием финансовой платформы // Российское право: образование, практика, наука. 2021. № 5. С. 29-35.

[171] Белоусов, А. Л. Теоретические и практические аспекты формирования финансового маркетплейса в Российской Федерации // Russian Journal of Economics and Law.2021. Т. 15. № 3. С. 413-424.

[172] Исмаилов И.Ш. Правовое регулирование финансовых платформ и маркетплейсов в контексте развития инструментов финансирования бизнеса: отечественный и зарубежный опыт // Финансовое право. 2022. № 11. С. 26-32.

[173] Федеральный закон от 20.07.2020 № 211-ФЗ (ред. от 04.08.2023) «О совершении финансовых сделок с использованием финансовой платформы» // Собрание законодательства РФ. 2020. № 30. Ст. 4737.

- оператор финансовой платформы;
- финансовые организации;
- эмитенты;
- потребитель финансовых услуг;
- регистратор финансовых транзакций.

Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (также именуемый Законом о ЦФА) конкретизирует перечень субъектов, принимающих участие в функционировании информационных систем (ИС). К ним относятся оператор информационной системы, бенефициарный владелец, а также пользователи, среди которых выделяются узлы ИС и операторы обмена цифровыми финансовыми активами (ЦФА).

Эти субъекты можно сгруппировать следующим образом: во-первых, к операторам информационных систем относятся организации, осуществляющие управление цифровыми платформами; во-вторых, группа пользователей подразделяется на две подкатегории — бенефициаров и участников, относящихся к структурным элементам информационной системы; третью группу составляют субъекты, обеспечивающие инфраструктурную поддержку.

Российское законодательство подробно регулирует правовой статус и функционал операторов ИС. Согласно статье 13 Закона об информации, ключевая ответственность за администрирование такой системы возлагается либо на собственника, либо на специально уполномоченное лицо, с которым заключен договор, определяющий режим обработки информации, размещенной в базах данных.

Оператор информационной системы наделен не только обязанностями по управлению процессами, но также разрабатывает и реализует алгоритмы функционирования, поддерживает техническую устойчивость и обеспечивает актуализацию системных механизмов обращения с данными.

В итоге компетенции оператора информационной системы обширно влияют на комфорт и безопасность взаимодействия каждого пользователя системы, определяя не только технические характеристики и возможности системы, но и права с обязанностями, возложенными на всех ее участников.

Ключевую роль в управлении и обеспечении надлежащей работы информационной системы играет именно ее оператор. Этот субъект не только устанавливает фундаментальные понятия и основополагающие термины, но и разрабатывает регулятивные правила и критерии, которые диктуют условия для эффективного функционирования системы в целом.

Он устанавливает порядок присоединения к информационной системе, заключает договоры с участниками, обеспечивающими ее работу, и координирует все процессы, связанные с ее функционированием. Кроме того, оператор взаимодействует с различными регуляторами, осуществляя необходимую деятельность по налоговому, таможенному и валютному администрированию, а также обеспечивает надзор в области предотвращения отмывания доходов, полученных преступным путем, и финансирования терроризма (ПОД/ФТ). Таким образом, оператор информационной системы выполняет ключевую роль в обеспечении ее функционирования и соблюдении нормативных требований.

Физические лица, выступающие в роли потребителей информации, осуществляют свои права на доступ к информации через активное взаимодействие с различными источниками, такими как сеть «Интернет», печатные СМИ, телевизионные и радиовещательные каналы. Их права распространяются не только на возможность находить и получать информацию, но и на ее использование в соответствии с их потребностями. Ключевым аспектом является доступ к информации, которая должна быть не только доступной, но и актуальной, проверенной и качественной. Кроме того, право на личную конфиденциальность и защиту персональных данных является фундаментальным, гарантируя сохранность личной информации каждого индивида.

Физические лица, выступая в роли создателей информации, пишут статьи, создают информационный контент, фотографируют, снимают видео или

разрабатывают программное обеспечение. В этой роли физические лица как субъекты информационных правоотношений обладают правами интеллектуальной собственности, такими как авторские права, и могут контролировать использование и распространение своих творческих работ. Физические лица как пользователи информационных систем взаимодействуют с информацией, делятся информацией, комментируют и оценивают контент, участвуют в онлайн-дискуссиях и других активностях, связанных с информацией. Физические лица могут осуществлять защиту прав путем обращения в суд или к регулирующим органам, если считают, что их права на получение качественной информации или защиту личных данных были нарушены. В этой роли физические лица как субъекты информационных правоотношений могут способствовать соблюдению законодательства и стандартов в сфере информации.

Органы государственной власти, как субъекты информационных правоотношений, обладают определенными правами и обязанностями, в том числе имеют право на доступ к информации, необходимой для осуществления своих функций, и право на использование информации в соответствии с законодательством, одновременно несут обязанности по предоставлению информации, обработке и хранению информации, защите информации и соблюдению законодательства в сфере информации[174].

Отдельное место среди субъектов информационно-правового обеспечения занимает АНО «Цифровая экономика». Целью данного субъекта является оказание услуг в сфере развития цифровой экономики, в том числе путем поддержки общественно значимых проектов и инициатив в сфере, координации взаимодействия между бизнес-сообществом, научно-образовательными организациями, иными сообществами и органами государственной власти[175].

---

[174] В качестве примера обязанностей органов государственной власти по предоставлению информации можно привести Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации. 2009. № 7. Ст. 776.

[175] Устав Автономной некоммерческой организации «Цифровая экономика». URL: https://files.data-economy.ru/Docs/ustav_d-economy.pdf (дата обращения: 02.03.2025).

В рамках вертикали власти созданы Правительственная комиссия по цифровому развитию, использованию ИТ и улучшения качества жизни и условий ведения предпринимательской деятельности, Проектный офис Правительства РФ, Президиум комиссии по цифровому развитию, Подкомиссия по цифровой экономике, Министерство цифрового развития, связи и массовых коммуникаций РФ. Также, в зоне своей ответственности, в реализации Программы участвуют отраслевые ведомства (например, проект по внедрению искусственного интеллекта контролирует Минэкономразвития РФ, Роскомнадзор выполняет функции регулятора и надзорного органа в сфере связи, информационных технологий и защиты данных, регулирует обработку персональных данных, осуществляет блокировку запрещенного контента, поддерживает цифровую трансформацию государства).

Г.Г. Головенчик указывает на то, что юридические лица, участвующие в информационном процессе – это, прежде всего, цифровые транснациональные компании, а также компании-единороги[176].

В последние годы традиционные крупные компании, прежде всего в нефтегазовом секторе, были превзойдены компаниями, участвующими в создании глобальных цифровых экосистем, которые принято называть цифровыми гигантами. Четыре ведущих цифровых гиганта превратились в масштабные транснациональные монополии. Google контролирует 90 % поисковой рекламы, Apple является мировым лидером по продажам смартфонов, Facebook[177] контролирует 80 % мобильного трафика, а на долю Amazon приходится 75 % продаж электронных книг. Эти компании заняли доминирующие позиции на своих рынках, оказывая значительное влияние на цифровой ландшафт[178].

Появление цифровых гигантов и создание цифровых экосистем имеет как положительные, так и отрицательные последствия. С одной стороны, эти компании

---

[176] Головенчик Г.Г. Цифровая экономика [Электронный ресурс]: учеб.-метод. комплекс. Минск: БГУ, 2020. 1 электрон. опт. диск (CD-ROM).

[177] Принадлежит компании Meta, признанной экстремисткой и запрещенной на территории Российской Федерации.

[178] Цифровое будущее: кто будет рулить миром – национальные правительства или транснациональные корпорации. URL: https://www.hse.ru/news/expertise/442058357.html (дата обращения: 22.04.2025).

произвели революцию в промышленности, предоставили инновационные продукты и услуги, способствовали экономическому росту. С другой стороны, их функционирование может подавлять конкуренцию, ограничивать возможности потребителей и вызывать опасения по поводу конфиденциальности, безопасности данных.

Развитие цифровых технологий не только укрепляет позиции компаний-гигантов, но и порождает множество стартапов, которые стремятся стать такими же крупными, как представители BigTech. Многие из этих стартапов процветают на этом пути. Традиционно, компании, которые достигли оценки в 1 миллиард долларов, называют «единорогами».

Появление «единорогов» свидетельствует о стремительном росте и потенциале инновационных стартапов в цифровом секторе. Эти компании разрушают традиционные отрасли, внедряют новые бизнес-модели и привлекают значительные инвестиции. Более того, появилась новая категория компаний, чья стоимость превышает 10 миллиардов долларов, известных как «декакорны». Такие компании добились исключительного роста и рыночной стоимости, позиционируя себя в качестве основных игроков в своих отраслях. Некоторые «декакорны» даже достигли стоимости, превышающей 100 миллиардов долларов, что позволило им получить звание «гектакорнов».

Распространение «единорогов» и появление «декакорнов» подчеркивает динамичный характер цифровой экономики и потенциал разрушительных инноваций, а их успех демонстрирует важность создания среды, поддерживающей инновации, предпринимательство и доступ к капиталу. Правительства, инвесторы и отраслевые игроки внимательно следят за развитием событий и рассматривают стратегии, направленные на стимулирование и поддержание роста экосистемы цифровых стартапов.

В целом развитие цифровых технологий не только укрепило позиции компаний-гигантов, но и привело к появлению многочисленных стартапов, стремящихся стать следующими единорогами и декакорнами. Рост этих компаний свидетельствует о потенциале инновационных стартапов в цифровом секторе,

привлекающих значительные инвестиции и разрушающих традиционные отрасли. Мониторинг и понимание роста «единорогов» и «декакорнов» дает ценное представление о динамике развития цифровой экономики, а также о возможностях и проблемах, которые они представляют[179].

В сфере информационных правоотношений существуют специфические ситуации или роли, требующие особого регулирования, соответственно, наряду с субъектами информационных правоотношений формируются новые субъекты.

Помимо классических субъектов правоотношений, в цифровых правоотношениях можно выделить ряд специфических участников, к которым следует относить информационных посредников.

Категория «информационный посредник» появилась в России в 2013 году для обозначения субъекта ведущего посредническую деятельность по передаче, хранению или предоставлению доступа к информации (статья 1253.1 ГК РФ). Под информационными посредниками (далее – ИП) понимаются лица, которые осуществляют передачу материала в информационно-телекоммуникационной сети, в том числе в «Интернет»; предоставляющие возможность доступа к материалу в сети. Российский законодатель сознательно отказался от понятий «провайдер хостинга», «провайдер».

Стоит сказать, что нынешняя группировка ИП не дает эвентуальности односложно размежевать их по видам.

Можно сформулировать логический конструкт группировки исходя из их деятельности:

1. ИП, осуществляющие передачу информации или предоставляющие доступ к ней;
2. ИП, занимающиеся кэшированием;
3. ИП, ограничивающие доступ к информации для пользователей;

---

[179] Единороги, декакорны и гектакорны: как финтех-индустрия ставит рекорды роста. URL: https://www.forbes.ru/finansy/439263-edinorogi-dekakorny-i-gektakorny-kak-finteh-industria-stavit-rekordy-rosta (дата обращения: 02.03.2025).

4. ИП, осуществляющие поиск информации[180].

В России существует две классификации ИП. Первая, вытекает из ст. 17 Закона об информации[181], регулирующая публично-правовую ответственность:

– лиц, осуществляющих деятельность по передаче информации, предоставленным другим лицом;

– лиц, осуществляющих деятельность по хранению информации и обеспечению доступа к ней.

Вторая (более обширная) вытекает из ст. 1253.1 ГК РФ:

– ИП, осуществляющие передачу информации (п. 2);

– ИП, предоставляющие эвентуальность размещения материала (п. 3);

– ИП, предоставляющие эвентуальность размещения информации, нужной для получения материала (п. 1);

– ИП, дающие эвентуальность доступа к материалу (п. 5)[182].

ИП сами не инициируют обмен данными. ИП участвуют в общественных отношения, относящихся к предмету информационного права, поэтому могут выступать как самостоятельные акторы. ИП самостоятельно осуществляют триаду, образующую статус[183]. Легальный статус формируется сразу двумя нормативными правовыми актами – частью четвертой ГК РФ и Законом об информации. Подобная специфика правового воздействия объясняется тем, что ГК РФ регулирует деятельность ИП в сфере интеллектуальных прав, Закон об информации в отношении всех иных правоотношений[184]. Однако данный подход соблюдается не полностью: Закон об информации, отчасти, регулирует отношения ИП и в области интеллектуального права. Так, ст. 15 регулирует обязанность провайдеров хостинга и провайдеров услуг доступа к «Интернету» по ограничению доступа к

---

[180] Данная классификация позволяет более точно регулировать права, обязанности и ответственность информационных посредников в зависимости от определенного вида деятельности, который они осуществляют.

[181] Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

[182] Необходимо сделать оговорку – ст. 1253.1 ГК РФ явно не называет данных лиц в качестве ИП, но указывает, что в отношении этих лиц распространяется правила статьи.

[183] Имеются в виду права, обязанности и ответственность.

[184] Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (постатейный). М.: Статут, 2015. 320 с.

информации, размещенной с нарушением интеллектуальных прав. Эта же норма регулирует внесудебную процедуру, в соответствии с которой владельцы сайтов (которые также могут быть ИП) должны предпринимать меры по прекращению нарушений авторских и смежных прав после получения заявления от правообладателя.

Как мы видим, регулирование ИП является противоречивым и создает неопределенность. Так, Закон об информации в ст. 15.2 и ГК РФ в п. 3 ст. 1253.1 ГК РФ регулирует обязанность ИП по удалению и ограничению доступа к информации, размещенной с нарушением авторских прав. Но, так как ни одна из норм не ссылается друг на друга, то наблюдается правовая коллизия.

Доктринальные источники справедливо подчеркивают, что, анализируя правовое регулирование участников информационного пространства, необходимо провести грань между их первичным статусом в качестве элементов реальных социальных взаимодействий и теми особенностями этого статуса, которые формируются под влиянием цифровизации отношений. Эксплуатация информационных систем предполагает активность операторов в качестве медиаторов, которые олицетворяют собой важнейший канал в претворении и управлении такими общественными связями[185].

Также в некоторых работах можно встретить идею о «квазисубъектах» права и споры о наличии у них правосубъектности, так называемые «юниты искусственного интеллекта»[186].

Введение в научный оборот понятия квазисубъектов в области правовых отношений, согласно взглядам экспертов, способствует более четкому разграничению статуса и функций различных участников, а также формированию адекватного комплекса их прав и обязанностей. Благодаря этому становится возможным организовать стабильную и сбалансированную работу правовых механизмов. Квазисубъектами информационно-правовых взаимоотношений

---

[185] Попондопуло В.Ф. Правовые формы цифровых отношений // Юрист. 2019. № 6. С. 29–36.

[186] Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. № 2. С. 36-55.; Морхат П.М. Концепт «электронного лица» в классификации субъектного состава лиц в гражданском праве // Пермский юридический альманах. 2019. № 2. С. 273-282.

принято называть таких лиц и организации, которые формально не обладают всем спектром характеристик полного субъекта права, однако наделены определенными юридическими возможностями и ответственностями в соответствующем сегменте. В число указанных квазисубъектов принято относить, например, информационных посредников, отдельные неправительственные структуры, зарубежные организации без статуса юридического лица по иностранному законодательству, а также транснациональные корпоративные объединения и другие подобные участники[187].

Наиболее яркой темой выступает возможность признания программы с элементами искусственного интеллекта в качестве субъекта правоотношений. Существуют прецеденты получения роботом гражданства[188], предоставления чат-боту резидентства[189], получение искусственным интеллектом патента[190], конечно, данные прецеденты носят репутационный характер, но порождают вполне реальные правовые последствия. Возникающие проблемы можно разделить на две группы: установление необходимого правового режима соответствующей программы и предупреждение последствий. Спецификой моделей искусственного интеллекта выступает то, что с определенного момента модель начинает обучаться самостоятельно. Это отличает модели от программ для ЭВМ: объект по истечении времени изменяет себя, меняется его коммерческая стоимость, отсюда вытекает вопрос, что мы защищаем, исходный код или результат? Вопрос возникает в сфере субъектного состав, кто ответственный субъект: разработчик, владелец ресурса[191],

---

[187] Чубукова С.Г. Квазисубъекты в киберправе // Вестник Университета имени О.Е. Кутафина. 2023. № 2 (102). С. 53-61.

[188] Человекоподобный робот получил гражданство Саудовской Аравии. [Электронный ресурс]. URL: https://www.techinsider.ru/technologies/news-393732-chelovekopodobnyy-robot-poluchil-grazhdanstvo-saudovskoy-aravii/ (дата обращения: 02.03.2025).

[189] ИИ Официально получил вид на жительство и ожидает защиты своих прав. [Электронный ресурс]. URL: https://robogeek.ru/iskusstvennyi-intellekt/ii-ofitsialno-poluchil-vid-na-zhitelstvo-i-ozhidaet-zaschity-svoih-prav (дата обращения: 02.03.2025).

[190] ЮАР выдала ИИ-системе первый в мире патент на изобретение. [Электронный ресурс]. URL: https://d-russia.ru/juar-vydala-ii-sisteme-pervyj-v-mire-patent-na-izobretenie.html (дата обращения: 02.03.2025).

[191] Ролинсон П., Ариевич Е.А., Ермолина Д.Е. Объекты интеллектуальной собственности, создаваемые с помощью искусственного интеллекта: особенности правового режима в России и за рубежом // Закон. 2018. № 5. С. 63-71.

пользователь или программа как субъект[192] либо не защищать вовсе[193]? Существует несколько подходов к вопросу правового режима программного обеспечения, рассмотрение которых представляется интересным:

– формальный, по нему субъектами являются юридические лица и физические лица;

– концепция «плода», высказывается идея о приравнивании к вещам, создаваемыми вещами[194];

– приравнивание к правовому положению животных[195];

– технический подход, связанный с идеей «электронного лица», с ограниченной правосубъектностью[196].

Последний подход указывает на изменение статуса программы, так как она способна к самообучению и, по сути, программа становится квазисубъектом. Если мы говорим о моделях ответственности, то они могут строиться на:

– наложении обязательств по страхованию рисков на первоначального собственника;

– использование модели ответственности раба, известной римскому праву;

– определению лиц, ответственных за причиненный вред.

Если мы рассуждаем о том, кого наделять правомочиями на результат, то большинство авторов утверждают, что владельцем прав на первичный и производный результат выступает создатель программы либо владелец прав[197].

---

[192] Abbott R.I Think, Therefore I Invent: Creative Computers and the Future of Patent Law // Boston College Law Review. 2016. Vol. 57. P. 1112-1114.

[193] Войниканис Е.А., Семенова Е.В., Тюляев Г.С. Искусственный интеллект и право: вызовы и возможности самообучающихся алгоритмов // Вестник Воронежского государственного университета. Серия: Право. 2018. № 4. С. 137-148.

[194] Гурко А. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 12. С. 7-18.

[195] Архипов В.В., Наумов В.Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. 2017. № 5. С. 157-170.

[196] Мохат, П. М. Концепт «электронного лица» в классификации субъектного состава лиц в гражданском праве // Пермский юридический альманах. 2019. № 2. С. 273-282..

[197] Витко В. Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // Интеллектуальная собственность. Авторское право и смежные права. 2019. № 2. С. 5-22.; Гаврилов Э.П. Советское авторское право: основные положения, тенденции развития. М.: Наука, 1984. С. 37.; Синельникова В.Н., Ревинский О.В. Права на результаты искусственного интеллекта // Копирайт. 2017. № 4. С. 22-23.; Куликова Е.В. Влияние новых технологий на развитие авторского права и смежных прав: договоры, законодательство, практика: автореф. дис. … канд. юрид. наук: 12.00.03. М., 2001. С. 12.

Реализация данной идеи представляется преждевременной, так как порождает огромное количество неразрешенных проблем и выявляет неготовность законодательства к изменениям, для ее реализации потребуются колоссальные изменения, однако изучение и моделирование потенциальных способов решения задачи представляется интересным в рамках диссертационного исследования.

Принятие законов о программах искусственного интеллекта частично связано с узакониванием информации в качестве предмета гражданских правоотношений. С одной стороны, данные можно воспринимать как форму информации. С другой стороны, информация, обладающая экономической стоимостью в контексте искусственного интеллекта, может быть отнесена к специальной категории программ для компьютеров.

Стоит уделить внимание относительно новой категории — «электронному лицу»[198]. Правовая специфика электронных лиц усложняет понимание и определение юридически значимого поведения в сфере электронных коммуникаций и трансакций. Электронные лица представляют собой субъектов, взаимодействующих и осуществляющих свою деятельность в сети «Интернет» или других электронных средах.

Уникальность правового положения так называемых «электронных лиц» обусловлена спецификой их функционирования и характера взаимоотношений, возникающих при их участии. В этих условиях становится актуальной задача формирования новых правовых механизмов, способных адекватно отражать особенности статуса электронных лиц и гарантировать их интересы.

Для того чтобы юридическая система могла эффективно реагировать на вызовы, связанные с применением и развитием высокоинтеллектуальных автономных систем, потребуется разработка оригинального комплекса норм и установление соответствующих процедур регулирования. Новая нормативная база должна позволить разрешать юридические коллизии, возникающие при появлении

[198] Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права Российской академии наук. 2018. Т. 13. № 2. С. 36-55.

субъектов, обладающих свойствами, присущими «сильному» искусственному интеллекту.

Правовая категория «электронные лица» достаточно широко представлена с точки зрения правосубъектности данных участников информационных правоотношений в работах О.А. Ястребова. Права и обязанности электронных субъектов могут быть сформированы в соответствии с моделью, основанной на теории Г. Кельзена, в рамках которой электронный субъект может быть интерпретирован как персонифицированное единство правовых норм, связывающих и наделяющих искусственный интеллект критериями «разумности». Электронный субъект может выполнять ряд функций в соответствии с целями, определенными разработчиком искусственного интеллекта, выступая в качестве действующего субъекта, поскольку принимает на себя обязательства, которые он может выполнить или нарушить. В связи с этим возникает вопрос о том, кто будет нести ответственность за неисполнение этих обязательств — сам электронный субъект или разработчик искусственного интеллекта. В настоящее время в России ответственность за противоправные последствия функционирования промышленных роботов возлагается на их владельцев, производителей или операторов. Важно отметить, что правовая база, касающаяся электронных устройств и искусственного интеллекта, продолжает развиваться и различается в разных юрисдикциях. Ответственность за действия и последствия использования электронных устройств может регулироваться специальным законодательством, нормативными правовыми актами или договорными соглашениями. Во многих случаях ответственность может лежать на заинтересованных лицах, таких как разработчики, владельцы или операторы электронных объектов[199].

Распределение ответственности за действия электронных субъектов – сложный и многогранный вопрос, требующий тщательного рассмотрения, так как включает в себя правовые, этические и общественные соображения, в том числе вопросы подотчетности, ответственности и потенциального воздействия на отдельных людей и общество в целом. По мере развития искусственного

[199] Там же.

интеллекта будет продолжаться разработка нормативной правовой базы для решения этих вопросов и обеспечения ответственного и подотчетного использования электронных объектов. Заинтересованным сторонам, включая разработчиков, пользователей и политиков, крайне важно быть в курсе меняющегося правового ландшафта и участвовать в дискуссиях и сотрудничестве для создания соответствующих рамок, обеспечивающих баланс между инновациями, подотчетностью и защитой прав личности и интересов общества.

В качестве причин для наделения искусственного интеллекта правосубъектностью (ограниченной) перечисляют:

– моральное право акторов на правосубъектность;

– социальный потенциал актора;

– удобство с правовой позиции[200].

В качестве логического конструкта, при котором можно будет задуматься о полноценном внедрении данного субъекта, можно обратиться к работе С.М. Солеймена[201]. Данный конструкт позволит освободить создателей и пользователей от потенциальной ответственности за действия юнитов.

Возможно, сейчас рано об этом говорить, но учитывая тенденции по развитию машинного обучения, и переходу его к «сильной» форме, нельзя игнорировать то обстоятельство, что технология искусственного интеллекта самообучается, соответственно, изменяется. Учитывая то, что государство обозначило одной из своих задач — развитие и интеграцию технологии искусственного интеллекта, вопрос ограничения моделей развития искусственного интеллекта представляет собой первоочередную задачу[202].

Наделение технологии искусственного интеллекта правоспособностью (полностью или частично) является спорным тезисом. С одной стороны, наделение

---

[200] Wietzenboeck E.M. Electronic Agent and the Formation of Contracts // International Journal of Law and Information Technology. 2001. Vol. 9. № 3. P. 204-234.

[201] Solaiman S.M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy // Artificial Intelligence and Law. 2017. Vol. 25. № 2. P. 155-179.

[202] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.; Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства Российской Федерации. 2020. № 35. С. 5593.

ее правоспособности может привести к злоупотреблениям со стороны разработчиков. С другой стороны, игнорирование данного обстоятельства может привести к необратимым последствиям.

В качестве промежуточного решения можно сделать ряд предложений:

1. Строить модели развития искусственного интеллекта через принцип обучения с подкреплением, так как он позволяет адаптировать, автономизировать решение задач. Данное умозаключение обусловлено изучением различных видов машинного обучения. Обучение с учителем предполагает дозированное предоставление данных, где каждой выходной выборке будет соответствовать правильный ответ. В качестве ограничения выделяются: требование в объеме данных (большое количество «размеченных» данных); система не может действовать в условиях неопределенности или изменяющихся обстоятельств; пассивность системы, которая выражается в отсутствии взаимодействия с окружающей средой, система воспроизводит лишь предоставленные данные. Обучение без учителя предполагает поиск скрытых паттернов в данных без явных меток (уменьшении размерности). В данном случае к ограничениям можно отнести – отсутствие целевой функции (система не решает определенную задачу, она формирует структуру данных). Обучение с подкреплением (именно данная модель представляется наиболее релевантной) предполагает то, что агент учится через взаимодействие со средой, получая обратную связь в виде «награды» за действие. К преимуществам относятся: адаптивность, автономность модели (не нужны новые данные), генерализация (агент способен переносить знания в новые условия). В отличие от обучения с учителем, обучение с подкреплением без учителя – решает конкретные задачи через целенаправленное взаимодействие. Однако, учитывая наличие интеллекта у некоторых систем на уровне девятилетнего ребенка, этого недостаточно. Лучшим способом для построения регулирования является выборочное замедление общественного внедрения больших языковых моделей искусственного интеллекта.

2. В правовой плоскости необходима концепция регулирования применения искусственного интеллекта международного характера, имеющихся

актов недостаточно, особенно на национальном уровне. В первую очередь, в сфере ответственности.

В диссертационном исследовании стоит отразить тот факт, что концепция «электронного лица» отлична от концепции квазисубъектности искусственного интеллекта. Отличия проявляются в следующем: предполагается, что «электронное лицо» имеет полную автономию воли, оно само реализует свои права, высказываются идеи о наделении технологии искусственного интеллекта правом на функционирование, право на энергообеспечение и другие[203]. Данный подход требует изменения всей системы права.

Подход к технологии искусственного интеллекта как квазисубъекту с ограниченной правоспособностью предполагает наделение ее лишь некоторыми правами (аспектами правосубъектности), например, наделение гражданско-правовой ответственностью за причиненный вред. Однако, на сегодняшний день, рано предлагать изменение подхода, данное предложение представляет собой лишь один из вариантов будущего взаимодействия с технологией искусственного интеллекта.

Систему субъектов информационно-правового обеспечения цифровой экономики можно разделить на две составные части: субъекты, поддерживающие функционирование информационной инфраструктуры и участников рынка цифровых продуктов и услуг. Технологию искусственного интеллекта, на сегодняшний день, рано относить к категории субъектов (квазисубъектов), уместнее рассматривать ее как источник повышенной опасности.

[203] Баловсяк Н. Право на убийство: есть ли у людей право уничтожать роботов. URL: https://uip.me/2017/05/people-vs-robots/ (дата обращения: 05.06.2025).

ГЛАВА 2. ИНФОРМАЦИОННОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

§ 2.1. Российское информационное законодательство в области обеспечения цифровой экономики

Цифровая трансформация всей экономической системы становится основополагающим фактором благосостояния всех участников мирового хозяйства. Цифровые технологии, применяемые в различных сферах деятельности направлены на развитие социальной сферы, улучшение здоровья в сфере здравоохранения, получение доступной информации в сфере образования, развитие партнерских связей в коммерческой сфере и так далее[204].

Обработка больших массивов данных и применение результатов анализа разительно увеличивает эффективность экономических процессов[205].

Прежде, чем рассматривать отдельные проблемные страты, необходимо заострить внимание на необходимом элементе цифровизации общественных отношений, который способен облегчить взаимосвязь – технической возможности интероперабельности. Принцип интероперабельности является важнейшим факторов развития права в условиях инновационной экономики, в частности развития Интернета вещей[206], систем «умного» города. На сегодняшним день данный принцип вышел за рамки технической плоскости и учитывается при построении социальной системы взаимодействия.

---

[204] Ишеков К.А., Бокова Л.Н. Правовое регулирование использования информационных технологий в сфере образования // Конституционное и муниципальное право. № 1. 2025. С. 45-48.; А.Н. Цифровизация как механизм развития конкуренции на отраслевых товарных рынках (на примере рынка электроэнергии) // Бизнес, менеджмент и право. № 2. 2023. С. 38-44.; Колюшин Е.И. Инновационные технологии избирательного процесса в свете верховенства закона // Правосудие. № 3 (3). 2021. С. 124-150.

[205] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

[206] Burleson W., Carrara S. (eds.) Security and Privacy for Implantable Medical Devices. Berlin: Springer, 2014. 205 p.

В России понятие «интероперабельность» содержится в национальном стандарте[207].

Интероперабельность является ключевым атрибутом открытых информационных систем, осуществляемым с помощью внедрения унифицированных стандартов. Это свойство позволяет нескольким системам или их компонентам не просто делиться информацией, но и эффективно использовать полученные данные в ходе такого взаимодействия[208].

Выделяют четыре уровня интероперабельности: правовой, организационный, семантический и технический[209].

Под организационным понимается структурирование деятельности субъектов информационного обмена по общим моделям поведения. В данном плоскости помогают соглашения о взаимопонимании и взаимообслуживании.

Под семантическим уровнем понимается точность и удобство восприятия обмениваемой информации.

Технический уровень включает спецификации к интерфейсу, сервисы интеграции данных и другое.

Правовой уровень предполагает эвентуальность субъектов (в первую очередь, государственных органов), применяющих разные правовые основания, взаимодействовать между собой для обмена. Работа на данном уровне начинается с систематизации нормативной базы на предмет установления барьеров.

К правовым средствам, способствующим внедрению интероперабельности, относятся стандартизация и техническое регулирование, правовые требования к открытости, технологической нейтральности и информационной безопасности.

Одной из ключевых проблемных страт сферы систематизации и кодирования информации является проблема дублирования данных в различных

---

[207] Национальный стандарт Российской Федерации ГОСТ Р 55602-2012 Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. 2012. URL: https://docs.cntd.ru/document/1200102958.

[208] Там же.

[209] Inter-organisational e-government: From four levels of interoperability to seen dimensions of co-gjvernance. 2015. URL: https://www.diva-portal.org/smash/get/diva2:783907/FULLTEXT01.pdf. (дата обращения: 29.07.2025); Malta National ICT Interoperability Framework. 2019.

информационных системах. Для разрешения данной ситуации необходима регламентация процесса взаимодействия информационных ресурсов разных типов, систематизации и кодирования информации в них.

Принципы интероперабельности:

– транспарентность;
– многоцелевое использование IT-решений и данных;
– соблюдение информационной безопасности;
– технологической нейтральности;
– и другие.

Отдельные виды информации могут потребовать определения особых подходов к интероперабельности, включая персональные данные.

Внедрение унифицированных методик и стандартов в процедуры сбора, сохранения, анализа и передачи информации способствует достижению интероперабельности. Это касается не только информационных систем в целом, но и улучшает согласованность самих данных. Гармонизация процессов на всех этапах работы с информацией – ключ к эффективной коммуникации между различными платформами и обеспечению их совместимости.

Инструментарием выступает стандартизация. Дальнейшее развитие правового обеспечения интероперабельности подразумевают разработку и утверждение стандартов/спецификаций в сфере информационного обмена, развитие принципов открытости, транспарентности, доступности и других принципов.

Для повышения эффективности информационно-правовых механизмов в сфере цифровой экономики актуальным представляется введение принципа правовой интероперабельности.

Суть данного принципа заключается в том, что государственные структуры и коммерческие организации должны не только иметь возможность, но и нести обязанность координировать свои действия, обеспечивать взаимный обмен знаниями и данными в четко определенных регулируемых рамках. Такой подход предполагает отсутствие произвольных барьеров для доступа и использования

необходимой информации, при условии строгого соблюдения установленного регламента взаимодействия. Формирование подобного принципа обеспечит прозрачность и предсказуемость информационного обмена, а также гармонизацию интересов всех участников цифровых правовых отношений.

В призме персональных данных необходимо уделить внимание «большим данным». Их значимость для государственного управления обозначена во многих докладах Минцифры России, Минэкономразвития России и других ведомств. Так, в докладе Аналитического центра при Правительстве РФ приведено множество примеров использования больших данных в российской практике государственного управления[210]. Подчеркивается, что на сегодняшний день уже функционируют несколько систем (например, ЕСИА, портал «Госуслуг» и портал «Работа в России»), основанных на применении данной технологии[211]. Так как важность технологий отмечается большим количеством экспертов, признается официальными лицами, уже активно используется в государственном управлении и имеет множество перспектив, то их степень влияния получается самой высокой.

Термин «большие данные» представляет собой метафору, поскольку это понятие охватывает различные аспекты сбора, обработки и анализа больших объемов информации, что затрудняет его точное и универсальное определение. Учитывая сложность определения категории, А.В. Минбалеев акцентирует внимание на том, что большие данные можно рассматривать как сложный объект, включающий в себя и большие массивы данных, информационные технологии, используемые для их обработки, в том числе через сеть «Интернет» и иные информационно-телекоммуникационные сети[212]. В связи с этим, правовое регулирование в этой сфере не имеет единой модели, а опирается на подходы, выработанные в других правовых режимах информации, таких как защита персональных данных.

---

[210] Доклад Аналитического центра при Правительстве РФ «Большие данные для государственного управления: опыт внедрения (пилотное исследование). URL: https://ac.gov.ru/files/content/10087/sorokin-kruglyj-stol-issledovanie-pdf.pdf?ysclid=lsofph8lfv464938404 (дата обращения: 02.03.2025).

[211] Там же.

[212] Минбалеев А.В. Правовая природа больших данных // Вестник ЮУрГУ. Серия «Право». 2024. Т. 24, № 3. С. 88-93.

В мире принято различать два подхода к законодательному контролю над процессами обработки «больших данных»: это подходы, принятые в Европе и Соединенных Штатах Америки[213]. В фокусе европейского регулирования - гарантии уважения и защиты прав индивидов в контексте работы с массивами больших данных. Эта модель акцентирует внимание на обеспечении приватности и защите личных данных при взаимодействии с подобными технологиями.

Она акцентирует внимание на защите частной жизни и прав граждан, включая оценку воздействия технологий на эти права. Европейская модель предполагает строгие нормативные рамки для защиты персональных данных и обеспечения прозрачности при использовании данных.

Подход к регулированию обработки массивов данных в Соединенных Штатах отличается отсутствием единого комплексного законодательства. Большинство споров по вопросам приватности разрешается посредством судебных процедур, а контроль за использованием информации выстраивается преимущественно на уровне корпоративных регламентов и механизмов саморегулируемых организаций. Система ориентирована прежде всего на поддержание благоприятных условий для функционирования национальных IT-компаний, а также на формирование внутренних корпоративных правил для управления потоками данных.

В России система правового регулирования работы с большими данными находится на стадии активного становления. В настоящий момент ведется разработка отечественных стандартов и прорабатываются подходы к управлению технологиями, связанными с обработкой крупных информационных массивов и развитием искусственного интеллекта. Ведущая задача этих инициатив – сформировать нормативную основу, которая одновременно обеспечит высокий уровень защиты персональных сведений и будет способствовать продвижению технологического прогресса в русле государственных приоритетов[214].

---

[213] Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / М.О. Дьяконова, А.А. Ефремов, О.А. Зайцев и др.; под ред. И.И. Кучерова, С.А. Синицына. Москва: ИЗиСП, НОРМА, 2022. 376 с.

[214] Национальный стандарт ГОСТ Р ИСО/МЭК 20546-2019 «Информационные технологии. Большие данные. Обзор и словарь»; ГОСТ Р ИСО/МЭК 20546-2021.

Для правового регулирования «больших данных» и технологии обработки «больших данных» разумнее использовать гибридную модель, включающую стимулирующие меры для сферы.

Обсуждение основополагающих аспектов регламентации сектора «больших данных», исключая личностные информационные массивы, занимает значимое место в правовой сфере. В этом контексте особое внимание уделяется законодательным инициативам, облегчающим самостоятельное создание субъектами цифровой экономики норм и процедур для эффективного и прозрачного обмена данными.

Равно важно стремление к соблюдению справедливого равновесия между необходимостью открытого доступа к информационным накоплениям, собираемым государственными учреждениями, и условиями их всестороннего использования без предвзятости и ограничений.

Прогресс национальных предприятий в данной области тесно связан с выработкой и реализацией мер поощрения и поддержки, формирующих благоприятный климат для инноваций и развития.

Кроме того, актуальной задачей является установление особых правовых условий для проведения экспериментов и исследований в сфере «больших данных», позволяющих разрабатывать и тестировать передовые подходы и технологические решения.

Проблема «больших данных» связана с защитой персональных данных, используемых в составе «больших данных», обусловлена действиями самих субъектов персональных данных, которые публикуют личную информацию в общедоступных ресурсах, что создает цифровой след субъекта[215].

Термин «большие данные» обретает разные значения в зависимости от контекста его применения. Изначальное толкование, уделяющее внимание технической стороне вопроса, было представлено и зафиксировано в словаре

---

[215] Терещенко Т. Что думает законодатель о больших пользовательских данных? URL: https://zakon.ru/blog/2018/10/27/chto_dumaet_zakonodatel_o_bolshih_polzovatelskih_dannyh (дата обращения: 02.03.2025).

терминов компании Gartner[216]. Аспекты технической природы «больших данных» получили свое развитие и отражение в ряде отраслевых стандартов, подчеркивающих их структуру, особенности обработки и возможности хранения[217].

Л.Ю. Василевская определяет понятие «большие данные» как интегрированный комплекс информационного содержания и сопутствующих технологий. В числе этих технологий выделяются разработки в области искусственного интеллекта. Они находят широкое применение в различных процессах: начиная от поиска и аккумуляции информации до ее систематизации, обработки и распространения, а также в задачах оптимизации работы с базами данных[218].

А.И. Савельев подходит к пониманию «больших данных» как к динамично изменяемому набору информации. Особую ценность такие данные приобретают благодаря своей объемности и возможности быстро и эффективно обрабатываться автоматизированными системами, что позволяет выявлять в них новые уровни знаний и оптимизировать процессы принятия решений[219].

С технологической точки зрения, для характеристики «больших данных» применяется специализированная модель, известная как «множество V». Ключевые атрибуты этой модели включают в себя: объем данных (Volume), скорость их обработки (Velocity), разнообразие типов и форматов данных (Variety), изменяемость данных со временем (Variability), их точность и надежность (Veracity), а также сроки жизни данных (Volatility). Эти параметры служат для оценки сложности и выявления специфических особенностей обращения с большими объемами информации в разнообразных сферах применения.

---

[216] Big Data. URL: https://www.gartner.com/en/informationtechnology/glossary/big-data. [Электронный ресурс]. (дата обращения: 27.07.2023).

[217] ГОСТ Р ИСО/МЭК 20546-2021 «Национальный стандарт Российской Федерации. Информационные технологии. Большие данные. Обзор и словарь» (утв. и введен в действие приказом Росстандарта от 13.07.2021 № 632-ст). М.: Стандартинформ, 2021.

[218] Василевская Л.Ю., Подузова Е.Б., Тасалов Ф.А. Цифровизация гражданского оборота: big data в механизме гражданско-правового регулирования (цивилистическое исследование): монография: в 5 т. Т. 5 / отв. ред. Л. Ю. Василевская. М.: Проспект, 2023. С. 13-14.

[219] Савельев А.И. Направления регулирования больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122-144.

В рамках концепции «больших данных» могут использоваться как персональные данные, так и обезличенные, или их совокупность. Существует мнение, что данные, обезличенные или анонимизированные, должны рассматриваться как менее «чувствительная» информация, что открывает возможности для их неограниченной обработки[220].

А.В. Лисаченко в своих исследованиях обращал внимание на проблемы, связанные с геномными данными, подчеркивая риск их свободного обращения. По его мнению, несмотря на анонимизацию, существует несоответствие между потенциальными рисками использования геномной информации и реальной безопасностью, что делает необходимым введение ограничений на свободный оборот таких данных[221].

Определение правового режима «больших данных» затруднено их спецификой, а именно неоднородностью. Существует взгляд, согласно которому «большие данные» следует понимает как информационные услуги и признать их нетрадиционным объектом интеллектуальной собственности[222]. В таком случае, не ясен механизм защиты прав лица, реализовавшим эвентуальность обработки данных на законном основании.

Согласно точке зрения Л.Ю. Василевской, термин «big data» следует воспринимать как сложный, неделимый объект гражданских прав, который представляет собой единую технологию. В этом контексте «большие данные» можно уподобить базе данных. Поскольку в состав «больших данных» включены, или по крайней мере предполагается их включение, технологии искусственного интеллекта, существует основание для включения таких данных в перечень результатов интеллектуальной деятельности[223]. Учитывая, что базы данных уже находятся в перечне охраняемых объектов интеллектуальной собственности,

---

[220] Регулирование big data в России. URL: https://proright.ru/2018/12/03/bigdata/ (дата обращения: 02.03.2025).

[221] Лисаченко А.В. Правовой режим «больших геномных данных»: за и против свободного обращения // Российский юридический журнал. 2022. № 2. С. 140-151.

[222] Сергеев А.П., Терещенко Т.А. Большие данные: в поисках места в системе гражданского права // Закон. 2018. № 11. С. 106-123.

[223] Василевская Л.Ю., Подузова Е.Б., Тасалов Ф.А. Указ. соч. С. 18-19.

встанет задача устранения правовых противоречий, связанных с режимом защиты этих данных в рамках интеллектуальных прав[224].

С точки зрения А.П. Сергеева и Т.А. Терещенко, объемные информационные массивы не могут рассматриваться как объекты авторско-правовой охраны при их квалификации в качестве базы данных. Авторы подчеркивают, что действующие правовые инструменты, обеспечивающие защиту через институт смежных прав, не соответствуют специфике этих данных и не обеспечивают необходимый уровень регулирования. В результате становится очевидной потребность в формировании инновационного подхода к правовому урегулированию управления подобными информационными ресурсами, что обусловлено их особенностями и масштабами[225].

Получается, отнесение «больших данных» к базе данных не решает вопрос правового режима «больших данных». С формальной точки зрения, определение «больших данных» не подпадает под определение базы данных.

В силу этого существует позиция, согласно которой «большие данные» не являются объектами исключительных прав[226].

Также затрудняет установление правовой природы «больших данных» эвентуальность понимания их в четырех плоскостях: как плату за услуги; фактор конкуренции; барьер входа (экспансии) на рынок; товар[227].

Учитывая общедоступный характер данных, после их размещения в сайте, существует эвентуальность их обработки третьими лицами. С точки зрения защиты сторон правоотношений, можно высказать идею о распространении института открытой неисключительной лицензии на использование данных.

---

[224] В качестве примера неоднозначного понимания сущностного наполнения категории «большие данные» можно привести решение Таганского районного суда г. Москвы от 01.07.2021 г. по делу № 2-2418/2021. Роскомнадзор подал иск к поисковому ресурсу «Глаз Бога». Согласно позиции ведомства, бот, специализирующийся на аккумулировании больших данных по физическим и юридическим лицам, использовал информацию из закрытых источников, хотя заявлял о том, что все данные, представленные пользователям, размещены в открытых базах, соответственно, факт вторжения в частную жизнь отсутствует. Судебный орган пришел к выводу, что данное заявление не отвечает действительности. Позиция ведомства была поддержана. Бот был включен в Реестр нарушителей прав субъектов персональных данных.

[225] Сергеев А.П., Терещенко Т.А. Указ. соч.

[226] Санникова Л.В., Харитонова Ю.С. Цифровые активы: правовой анализ: монография. М.: 4 Принт, 2020. 304 с.

[227] Блажеев В. В. Цифровое право : учебник / В.В. Блажеев, М.А. Егорова. - Москва : Проспект, 2020. С. 123.

Сформирование универсальных параметров для соглашений, которые будут регламентировать передачу данных между аппаратными средствами, принадлежащих разнообразным институциям, представляется рациональной задачей. Такие типовые условия послужат надежной основой для организации четкого и эффективного обмена информацией.

Рассматривая обезличенные информационные ресурсы как значимый элемент современной цифровой экономики, необходимо обозначить различные типы подобных данных с точки зрения их правового регулирования. Эти ресурсы можно подразделить на два класса: полностью анонимизированные, утрата связи которых с конкретным субъектом необратима, и псевдоанонимизированные, для которых сохраняется вероятность повторной идентификации личности. В первом случае, такие данные не попадают под определение персональной информации, поскольку восстановить личность человека невозможно. В то же время, если остается возможность обратного установления связи с субъектом, такие сведения продолжают оставаться в правовой категории персональных данных.

В этой связи представляется обоснованным ввести для операторов обязанность осуществлять комплексную оценку угроз повторной идентификации — например, анализировать, какие ресурсы, средства и временные затраты могут быть необходимы для восстановления идентифицирующей информации, исходя из особенностей конкретного массива данных и условий его обработки.

Кроме того, следует отметить важный аспект, связанный с высокими рисками информационной безопасности, обусловленными зависимостью поставок аппаратного обеспечения от иностранных производителей.

Проблематика связана с тем, что многие программные и информационные системы проектируются и производятся за пределами страны, что потенциально ставит под угрозу цифровой суверенитет и безопасность государства. Применение зарубежных ИТ-решений, в том числе программного обеспечения, может стать каналом для неавторизованного доступа к конфиденциальным данным, даже если эти системы защищены. Существуют угрозы, заложенные на стадии разработки ПО, которые находятся вне досягаемости традиционных средств защиты.

Такое положение дел мотивирует руководство России активизировать усилия по созданию собственных информационных продуктов и технологий. Эти меры направлены на гарантирование информационной безопасности и укрепление защиты государственного уровня. Разработка внутренних компетенций в сфере высоких технологий целевым образом поддерживается на государственном уровне, что свидетельствует о стремлении к усилению независимости и технологической суверенности[228].

Дальнейший анализ проблемы требует акцентирования внимания на феномене цифрового следа. Сбор и последующая аналитика информации о действиях пользователей, осуществляющих покупки через онлайн-платформы, дают возможность компаниям не только строить предположения о будущих покупательских интересах, но и совершенствовать организацию бизнес-процессов. Для крупных игроков электронной коммерции, таких как Alibaba, Amazon или eBay, характерным становится использование технологий, позволяющих спрогнозировать потенциальные покупки конкретного клиента. Это выражается в персонализированной адаптации поисковых алгоритмов, предварительном формировании рекомендаций и даже возможности заранее размещать наиболее вероятные к заказу товары на соответствующих складах, оптимизируя логистическую схему.

Проблемой в сфере правового регулирования цифрового следа является практически полное отсутствие в отечественном законодательстве специальных правовых норм, что может рассматриваться в качестве «нулевой фазы» в регламентации рассматриваемых общественных отношений. Возрастание количества пользователей сети «Интернет», увеличение времени, проводимого пользователями в этой информационно-телекоммуникативной среде, способствуют появлению легкодоступной информации о каждом пользователе, которая представляет какую — либо ценность. Такая информация может быть оставлена пользователем при использовании социальных сетей, мессенджеров,

---

[228] Сухаревская А. Незаметное государство. URL: https://www.vedomosti.ru/partner/articles/2019/12/19/819009-nezametnoe-gosudarstvo (дата обращения: 02.03.2025).

заполнении регистрационных форм на различных сайтах, использовании специализированных порталов (портал государственных услуг Российской Федерации, портал государственных услуг субъекта РФ и так далее).

В рамках кредитных организаций, данные, образующие цифровой след, участвуют в оценке клиента. Эти данные представляют ценность для прогнозирования заемщика. Анализ типа устройства, операционной системы, длительности посещения сайта, временных интервалов посещения сайта, дают эвентуальность определить кредитоспособность пользователя[229].

Социальные сети активно используют данные, чтобы формирующие цифровой след для понимания личных интересов пользователей «Интернета». Это участие в общественных объединениях, местонахождение, поведение.

Крупные компании аккумулируют сведения, которые могут помочь сформировать цифровую личность пользователя. Эти сведения выливаются в подсказки, в предложения контента и другое.

Выделяют два метода создания цифрового следа: *активный* и *пассивный.* Активный создается самим пользователем, который добровольно делится информацией. Пассивным является способ, когда аккумулируются данные, оставленные не специально или как итог работы программы.

В соответствии со ст. 8 Конвенции о защите физических лиц при автоматизированной обработке персональных данных (далее — Конвенция) устанавливается ряд дополнительных гарантий для субъекта данных[230]:

– лицо имеет право быть информированным о наличии автоматизированной базы данных, содержащей персональные данные, понимать главные цели такого файла и знать имя и адрес проживания или юридический адрес ответственного за файл;

---

[229] Berg, T., Burg, V., Gombović, A., Puri, M. On The Rise of FinTechs – Credit Scoring Using Digital Footprints (July 15, 2019). URL: https://www.fdic.gov/analysis/cfr/working-papers/2018/cfr-wp2018-04.pdf.; Michael J. Brennan Irish Finance Working Paper Series Research Paper № 12-18. URL: https://www.ssrn.com/index.cfm/en/michael-j-brennan-irish-finance-res/.

[230] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // СПС Консультант Плюс (дата обращения 04.01.2025).

– иметь возможность получить подтверждение того, сохраняются ли его личные данные в таком автоматизированном файле без необоснованных задержек или расходов, а также иметь доступ к этим данным в понятной форме;

– требовать корректировки или удаления своих данных в случае их обработки с нарушением законодательных норм, которые реализуют ключевые положения статей 5 и 6 данной Конвенции;

– использовать средства юридической защиты при отказе в подтверждении факта хранения данных, а также для исправления или уничтожения неправомерно обработанных данных.

В соответствии с п. 2 ст. 12 Конвенции участник обработки не должна запрещать или получать специальное разрешение на трансграничные потоки персональных данных, идущие на территорию другого государства для защиты частной жизни. Однако можно отступить от этого правила:

а) насколько это разрешено внутренним законодательством, которое содержит специфические положения касаемо определенных видов персональных данных или автоматизированных систем учета этих данных, основываясь на их особенностях, при условии, что такие положения не противоречат мерам защиты, предоставляемым законодательством другой Стороны;

б) когда передача осуществляется с ее территории на территорию государства, не являющегося Стороной настоящей Конвенции, через территорию другой Стороны, в целях недопущения такой передачи, которая позволит обойти законодательство Стороны, упомянутой в начале данного пункта.

Проблемой в исследуемой сфере является значительно малое наличие специальных правовых норм. Ключевым вопросом является неоднозначность и разносторонность категории «цифровой след».

Цифровой след может быть охарактеризован как информация, оставляемая пользователем в процессе использования интернет-сайтов или во время регистрации на различных веб-платформах[231].

[231] Berg, T., Burg, V., Gombović, A., Puri, M. On The Rise of FinTechs – Credit Scoring Using Digital Footprints (July 15, 2019). URL: https://www.fdic.gov/analysis/cfr/working-papers/2018/cfr-wp2018-04.pdf.

Р. Хадкинс подчеркивает, что под цифровым следом понимается набор данных, которые индивиды публикуют о себе или создают при их взаимодействиях с множеством интернет-ресурсов[232].

Для совершенствования законодательства необходимо использовать широкий подход к категории «цифрового следа», включающий риск-ориентированный подход (подход должен строиться из безопасного, целевого, срочного использования данных в обезличенной форме, с возможностью деанонимизации самим субъектом или на основании судебного акта). Под риск-ориентированным подходом в сфере регулирования цифровых следов предлагается понимать стратегию, при которой способы контроля и управления массивами данных фокусируются на уменьшении потенциальных угроз, в соответствии с оценкой вероятности и последствий их воплощения. Риск-ориентированный подход обладает рядом ключевых аспектов: 1) при внедрении данного подхода должны быть сформулированы метрики для оценки рисков, например, по видам данных (чувствительная информации, «критичная» - результаты медицинского обследования и анонимная аналитика); по потенциальным последствиям; 2) приоритезация мер (большая часть ресурсов направляются для защиты данных с наибольшим риском) – для высокого риска применяются методы шифрования, аудиты; для невысокого риска применяется базовые меры защиты (доступ через пуш-уведомление на телефон). Интеграция данного подхода позволит адаптироваться к новым технологиям, организации смогут самостоятельно оценивать потенциальные риски. К преимуществам использования риск-ориентированного подхода в сфере регулирования цифровых следов относятся: проактивность (предупреждение рисков вместо реагирования на инцидент), повышение эффективности (происходит оптимизация расходов на безопасность). Высокорисковые данные должны храниться в защищенных хранилищах с шифрованием (например, Azure Confidential Computing); локальные серверы для соблюдения национального законодательства. Среднерисковые данные – облачные

[232] Hudkins Ronald E. Your Digital Footprint: Password Protection Requirements. Paperback. June 12, 2014. URL: https://www.scribd.com/book/230559848/Your-Digital-Footprint-Password-Protection-Require-ments

хранилища с контролем доступа (Amazon S3), низкорисковые данные – децентрализованные системы или публичные облака с базовой защитой. Реляционные базы данных (MySQL) для структурированных данных; NoSQL (Cassandra) для неструктурированных или полуструктрированных данных; Блокчейн для аудита изменений; Edge-хранилища для данных, генерируемых IoT-устройствами. Срок хранения также отличается: минимизация сроков хранения, которые необходимы для достижения целей. Ответственность за обращение с данными необходимо разделять между компаниями, государственными органами и технологическими провайдерами. Организации, собирающие и обрабатывающие данные, должны нести ответственность за процедуру обезличивания. Технологические провайдеры и вендоры: поставщики программного обеспечивания и облачных сервисов предоставляют инструментарий для автоматизации обезличивания (токенизация, анонимизация). Третьи стороны и подрядчики – контрактные обязательства (обезличивание может быть предусмотрено договором). Государственные регуляторы – устанавливают требования к обезличиванию с помощью нормативных правовых актов. Пользователи (косвенная роль) – могут запрашивать удаление или анонимизацию своих данных с помощью нормативных правовых актов, однако техническая реализация возложена на организации. Среди методов обезличивания необходимо использовать псевдонимизацию; анонимизацию; агрегацию; генерацию синтетических данных.

Стоит отметить, что чаще всего пользователи предоставляют в социальных сетях, специализированных ресурсах информацию:

– об имени, фамилии, мобильном телефоне, адрес регистрации/жительства;

– об образовании, месте работы, занимаемом положении.

Пассивно аккумулируются данные:

– о поисковой системе;

– об устройстве.

Данные общественные отношения взаимосвязаны с:

– воплощение прав человека в киберпространстве (возможность «цифровой смерти», право забвения и других);

– защитой, обработкой, хранением, передачей сведений, образующих цифровой след;

– идентификацией личности.

Понятия «цифровая тень» и «цифровой след» отражают разное содержание явлений, связанных с накоплением и сохранением информации в онлайновой среде. Под цифровой тенью обычно понимают автоматическую фиксацию сведений, возникающих в процессе пользовательской деятельности в сети, причем эти данные зачастую остаются не востребованными и не оказывают непосредственного влияния на последующие процессы. В отличие от этого, цифровой след формируется сознательными действиями человека в интернете и может оказывать значимое воздействие, например, в области персональных рекомендаций, маркетингового анализа либо при оценке структуры потребительских предпочтений.

В свою очередь, термин «цифровой двойник» имеет иную смысловую нагрузку: под ним подразумевается комплексная и изменяемая цифровая копия материального объекта или целой системы. В отличие от тени или следа, цифровой двойник не только накапливает исторические данные, но и предназначен для имитации состояния, поведения и функционирования реального прототипа. Результатом внедрения данной технологии становится возможность прогнозирования неисправностей, оптимизации рабочих процессов и повышения эффективности оборудования, что особенно важно для отраслей промышленности, медицины и авиационной сферы[233].

Важно четко разграничивать эти концепции во избежание путаницы. Так, под «цифровым двойником» предпочтительно понимать виртуальные аналоги физических объектов в информационных системах. В то же время выражение «цифровая личность» может отсылать к самостоятельной виртуальной

[233] Валеева, Г. В. Цифровой след и цифровая тень в контексте цифрового образования // Гуманитарные ведомости ТГПУ им. Л. Н. Толстого. 2023. № 4 (48). С. 59-67.

идентичности, к примеру, аватару в цифровом пространстве, созданному как отображение реального объекта или лица[234].

В научных трудах присутствует концепция, представляющая цифровую идентичность как комплекс уникальных атрибутов, которые позволяют установить личность владельца данных. Однако связь между этими атрибутами и самой личностью часто не является очевидной. В качестве иллюстрации можно привести номер социального обеспечения, который служит средством для установления личности человека, но не отражает его персональные качества[235]. Этот аспект подчеркивает сложность вопроса идентификации субъекта данных в цифровом пространстве.

Вопросы, касающиеся сферы «цифровой личности», можно условно разделить на две группы: одна из них охватывает вопросы, связанные с цифровыми данными документов (например, результаты обследований), а другая – с виртуальной активностью субъекта. В сфере осмысления цифровой идентичности, определяемой как электронное представление удостоверяющих личность документов и других данных, несущих в себе информацию о личности, резонно утверждать о необходимости применения к таким данным правил защиты, сопоставимых с теми, что используются для физических документов. Несмотря на наличие дебатов касательно этого вопроса, преобладает мнение о том, что документы обладают свойствами имущественных прав[236].

Таким образом, методы обработки различных элементов цифровой идентичности человека должны быть адаптированы в зависимости от целей использования этих данных.

В области цифровизации документооборота можно рассмотреть стратегию, идентичную методам управления физическими документами, таким как паспорт, индивидуальный налоговый номер, трудовая книжка и медицинский полис. Это

---

[234] Цифровой двойник. URL: https://digitaltwin.ru/products/digital-twin/ (дата обращения: 02.03.2025).

[235] Abelson H. and Lessig L.: ‘Digital identity in Cyberspace’, White paper submitted for 6.805 / Law of Cyberspace: Social Protocols (Dec 1998).

[236] Никитин А.В. О правовом режиме бумажных документов // Российский юридический журнал. 2015. № 4. С. 75-80.

подразумевает создание цифровых версий этих документов с сохранением ключевых принципов доступности, надежности и конфиденциальности.

При применении этого подхода, важно учитывать, что каждый цифровой документ должен быть защищен соответствующими средствами шифрования и аутентификации, чтобы обеспечить его подлинность и предотвратить несанкционированный доступ. Именно так обеспечивается как сохранность личных данных, так и их актуальность и юридическая значимость в рамках цифровой среды.

Такая система требует внедрения сложных технических решений и стандартов, которые он устанавливает, что позволяет реализовать функции электронного документооборота, аналогичные привычным бумажным процедурам. Результатом станет ускорение и упрощение процессов идентификации и обработки документов, повышение их защищенности от фальсификаций и в то же время поддержание строгого контроля над конфиденциальной информацией.

В случае персональных данных необходимо строго соблюдать требования как российского, так и международного законодательства. Сведения о виртуальной активности пользователя, такие как поисковые запросы и прочие данные, собранные без его согласия, следует обрабатывать либо как персональные данные, либо, в случае их анонимизации для статистических исследований, как сведения, составляющие коммерческую тайну.

Концепция цифровой личности не является новаторской в смысле ее сути, она скорее представляет собой современный метод фиксации и систематизации существующих данных о человеке. Тем не менее, требуется адаптация законодательства для адекватного отражения правовых аспектов управления и защиты личных данных в цифровом формате. Под эгидой «цифровой личности» понимается набор данных, включающий как официальные сведения из государственных регистров, так и персонализированную информацию, например, финансовую историю и личные предпочтения, что позволяет однозначно идентифицировать индивида в информационных системах.

Регулятивные акты, связанные с цифровой экономикой России, включая разработку концепции цифрового профиля граждан и ряд других предложений в этой области, привели к формированию определенных направлений правового регулирования:

– определение категории цифрового профиля;

– установление правил обращения удостоверения личности гражданина, идентификаторов;

– регламентация процедуры предоставления доступа представителей органов государственной власти и отдельных организаций к цифровым профилям граждан и хозяйствующих субъектов;

– прописывание ответственности операторов персональных данных при обработке персональных данных с применение инфраструктуры цифрового профиля.

Организационные и технические основы функционирования цифрового профиля определяются подпунктами «а» и «б» пункта 3 Положения, регулирующего эксперимент по совершенствованию качества и взаимосвязанности сведений, размещенных в государственных информационных ресурсах.

Формирование эффективной нормативной среды для цифрового профиля способно значительно расширить возможности предоставления государственных и муниципальных сервисов — как физическим лицам, так и организациям, а также государственным институтам.

Прогрессивное правовое обеспечение в этой сфере открывает дополнительные пути повышения доступности, оперативности и эффективности взаимодействия субъектов с государственными структурами.[237].

Важным элементом инфраструктуры цифрового профиля, основанной на единой системе идентификации и аутентификации, может стать публичный реестр

[237] Постановление Правительства РФ от 03.06.2019 № 710 (ред. от 02.02.2024) «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (вместе с «Положением о проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах»). Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201906070031.

согласий субъекта данных о возможной передаче данных третьей стороне из цифрового профиля на конкретный срок. В реестре должны сохраняться согласия на передачу данных и цели передачи. Функции по ведению реестра предлагается возложить на Роскомнадзор, который помимо ведения реестра разработает форму согласия. В реестре должны содержаться данные о субъекте (его идентификатор, например, хешированные данные), список третьих лиц, кому разрешена передача, цели и сроки передачи, дата предоставления. Самой подходящей технологий для создания реестра представляется блокчейн и предоставлением доступа через аутентификацию (онлайн-платформа, интегрированная в портал государственных и муниципальных услуг, например)[238]. Собираться информация будет от разных участников–обрабатывающих данные – банки, страховые компании, социальные сети, государственные учреждения, которую в обязательном порядке должны запрашивать согласие в заявочной форме, с помощью направления запроса и подписанием электронной подписью.

Стоит отметить, что с возрастанием массива персональных данных, возрастает степень вмешательства в частную жизнь субъекта и повышения эвентуальности нарушения его прав[239]. Факт получения государством приватной информации можно рассматривать как нарушение положений ст. 21 Конституции РФ[240], также есть опасность дискриминации. Проблема связана с эвентуальными ошибками в алгоритмах и программах принятия решения либо неверной интерпретации результата обработки. Учитывая профилирование и анализ данных клиентов кредитных организаторов и сотовых операторов[241], законодательство не дает механизм информирования субъектов ни о факте профилирования, ни об использовании методов, ни об эвентуальных рисках мониторинга. Также отсутствуют право на оспаривание результатов или право на ознакомление.

---

[238] Рустамов П.А. Совершенствование правового регулирования использования цифрового профиля // Юридический мир. 2025. № 6 (342). С. 44.

[239] Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 52.

[240] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 25.12.1993. № 237.

[241] URL: https://bankiros.ru/news/mts-banki-i-kollektory-2391.

Институт профилирования в российском праве отсутствует, что порождает правовые пробелы.

Обсуждение использования цифровых профилей неизбежно приводит к рассмотрению целей, для которых предназначена информация, а также к возможностям доступа к данным различных запросивших сторон. Персональные данные в цифровых профилях могут использоваться для широкого спектра функций, от повседневного администрирования до целей, требующих более тщательной обработки, таких как статистический анализ, налоговое обложение или сбор информации для национальных безопасных интересов.

Современное законодательство, как правило, ограничивается общими рамками использования данных, акцентируя внимание на сборе информации для «необходимых целей» и на принципах волеизъявления и согласия со стороны граждан. Тем не менее, точные механизмы, правила раскрытия данных и условия для конкретных примеров использования зачастую остаются без детализации. Это требует дополнительных уточнений и усовершенствования нормативной базы, чтобы обеспечить не только эффективность и удобство в использовании цифровых профилей, но и строгую защиту конфиденциальности и регулирование вопросов приватности.

Создавая рамки для допуска к персональным данным и определяя сферы их применения, законодатель должен учитывать баланс интересов общества и права каждого индивида на конфиденциальность и защиту его личной информации. Это включает в себя четко очерченные условия, при которых информация может быть передана третьим лицам, а также ограничения на объем и виды данных, которые могут быть доступны в определенных контекстах.

Более разумным подходом было бы ограничение предоставления данных до минимально необходимого объема для конкретной задачи или процедуры.

Можно сказать, что положения ч. 1 ст. 24 Конституции РФ охраняют данные граждан, однако ширина категории «частная жизнь»[242] и отсутствие легальной

[242] Конституционный суд РФ понимает под частной жизнью «область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит непротивоправный характер» (определение от 28.06.2012 № 1253-О).

регламентации обращения персональных данных для целей профилирования создают дополнительные риски[243]. Возможно, данные могут использоваться для противоправных действий со стороны государства или хозяйствующих субъектов (например, слежка за политической оппозицией).

В соответствии с ч. 3 ст. 5. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[244] строго запрещается слияние баз данных, если они не предназначены для совместной обработки информации. Однако это правило не применимо к цифровым профилям, поскольку в этом случае информация не объединяется в одну базу; данные перемещаются между разными информационными системами и извлекаются по мере надобности. Тем не менее, даже если базы данных фактически не объединены, то массив данных, который передан в центр персонализации, может рассматриваться как интегрированный[245].

Наблюдается ряд пробелов в страте управления цифровыми профилями, где особенно значимо создание защитных мер для обеспечения прав человека в процессе обработки данных. Необходимо ввести защитные механизмы для сохранения прав и свобод индивидуума от возможных отрицательных эффектов, связанных с агрегацией личной информации. В федеральном законе должны быть прописаны более конкретизированные гарантии неприкосновенности частной жизни в свете развития цифровых профилей. Необходимо исходить из принципа соразмерности наполнения массивами данных баз. Должна быть эвентуальность ограничения инкорпорации в профиль данных о «деликатной» информации (факты посещения врачей, судимости, о факте идентификации и аутентификации лица на сайтах с использованием ЕСИА). Установить перечень данных, которые будут храниться сепарировано от других и быть несвязанными (информация из системы геномной регистрации).

---

[243] Алимов Э.В., Малютин Н.С. Правовые позиции Конституционного Суда Российской Федерации по вопросам генетической истории семьи и суррогатного материнства. Журнал Белорусского государственного университета. Право. 2020. № 3. С. 1-8.

[244] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006 г. № 165.

[245] Чаннов С.Е. Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. 2018. № 9. С. 50-51.

Регламентация цифровых отпечатков, данных о местоположении и другой информации аналогичного характера должна основываться на методе, при котором во главу угла ставятся риски. Основная цель такого подхода – минимизация непредвиденных последствий для пользователя, которые не вызваны его добровольным согласием на использование его личной информации и прочей конфиденциальной информации[246]. В качестве возможного решения предполагается обязать анонимизировать такие данные с потенциальной возможностью возврата к первоначальному виду (деанонимизации) самим пользователем или по решению суда. Также целесообразным представляется установление ограничения на период хранения данных.

Дополнительно необходимо урегулировать вопрос цели и субъекта использования данных исходя из гарантий осуществления профилирования (указать невозможность цели использования данных для установления, например, политических взглядов, религиозных убеждений, философских концепций, информации об интимной жизни).

У гражданина должна сохраниться эвентуальность осуществления действий по реализации своих конституционных прав и свобод без использования цифрового профиля. Нельзя представлять цифровой профиль как единственным способ взаимодействия в правоотношениях.

Необходима правовая регламентация механизма уведомления заинтересованных лиц о факте профилирования и применяемых методах. Также необходимо право на ознакомление и оспаривание результатов профилирования, а объем предоставляемой информации должен быть минимален, без включения «деликатной» информации, обладающей особой значимостью для субъекта. Организации должны уведомлять пользователя о факте профилирования до или в момент сбора данных, если это может повлиять на его права (к примеру, отказ от предоставления услуги). Для уведомления о факте профилирования, можно использовать – всплывающее окно при первичном сборе данных, уведомление в

[246] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики (подготовлена некоммерческой организацией «Фонд развития центра разработки и коммерциализации новых технологий»). М., 2020. С. 17.

личном кабинете цифрового профиля, пуш-сообщение на почту; по запросу – отчеты на электронную почту либо использовать автоматическое триггерирование (уведомлять при изменении статуса, например, при отклонении заявки по результатам профилирования). С технической точки зрения, реализовать данную идею можно с помощью интеграции систем обработки данных (автоматическое уведомление при запуске профилирования) или API-связь с реестром согласий (данные о профилировании передаются в централизованный реестр, где пользователь их видит). Ответственность за уведомление о факте профилирования должны нести организации, осуществляющие обработку персональных данных, а в некоторых случаях – их партнеры. Контроллерами данных могут выступать компании, государственные учреждения, которые определяют цели и методы обработки данных (в перечень их обязанностей должны входить: уведомление пользователя о профилировании на этапе сбора данных, например, через политику конфиденциальности или прямое уведомление; продемонстрировать прозрачность логики и последствий профилирования, регистрировать факт профилирования в публичном реестре). При осуществлении этого действия должна быть тесная кооперация с обработчиками данных (третьей стороной, которая выступает посредником по поручению контроллера, например, облачные сервисы), в их обязанности должны входить: обязательное выполнение инструкций контроллера при уведомлении пользователей и оказание помощи контроллеру в подготовке уведомления (предоставлять технические данные об используемых алгоритмах). Ответственность представляется распределить следующим образом: контроллер будет ответственен за своевременное и понятное уведомление и интеграцию механизмов уведомления в систему; на обработчике будет лежать ответственность за техническую реализацию; регулятор (например, Роскомнадзор) будет отвечать за согласование правил уведомлений и применение санкций (например, 4 % за нарушение от оборота компании)[247]. Право на ознакомление и оспаривание

[247] Инструментарий оборотного штрафа известен российскому правопорядку. Для примера можно обратиться к Постановлению мирового судьи судебного участка № 422 по делу об административном правонарушении № 05-3220/422/2021 от 24.12. 2021. URL: https://mos-sud.ru/422/cases/admin/details/a600a573-e5a3-4629815c080f3c6220ed?caseDateFrom=&caseDateTo=&caseFinalDateFrom=&caseFinalDateTo=&caseNumber=&codex

результатов профилирования должно быть закреплено на трех уровнях: организационном, техническом и законодательном. На законодательном уровне изменения должны быть внесены в ст. 14 Федерального закона № 152-ФЗ «О персональных данных»[248], на организационном уровне, право должно быть зафиксировано в локальных правовых актах (в политике конфиденциальности должен быть раздел о профилировании с подробным описанием; в пользовательском соглашении – условия использования сервиса, где указано право на апелляцию). На техническом уровне – права реализуются через инструменты, доступные пользователям: личный кабинет – должна быть возможность подать запрос о разъяснении решения и оспаривания его.

К «деликатной» информации (использование, которой ограничено) относится чувствительные данные (отношение к религии, результаты медицинского обследования, информация о заболеваниях и прочее), а также избыточные данные (например, данные паспорта для персонализации рекламы). Минимизировать данные можно с помощью технологий анонимизации (заменить имя на идентификационный номер при сборе информации о поведении на сайте), агрегации (применять обезличивание при работе со статистическими данными), псевдоанонимизация (хранить данные в кодированном виде, где доступ имеется у контроллера). Для установления перечня минимума можно использовать оценку необходимости (если можно достичь цели без этих данных, тогда собирать их не нужно); через «privacy by design» (встраивать минимизацию данных в архитектуру системы на стадии разработки); через регуляторные рекомендации (следовать отраслевым рекомендациям и рекомендациям регуляторов в сфере обработки данных).

В призме цифровой экономики по целому ряду направлений законодательство нуждается в корректировки. В частности:

=&docsDateFrom=&docsDateTo=&documentStatus=&documentType=&hearingRangeDateFrom=&hearingRange (дата обращения: 02.03.2025).

[248] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006 г. № 165.

1. Определение правового режима новых видов информации (например, «больших данных»);

2. Корректировка правового режима персональных данных, в том числе обезличенных.

3. Разработка и инкорпорация унифицированных стандартов сбора, хранения, обработки, обмена данными («интероперабельность данных»). Концепция интероперабельности (переводимости) данных предполагает формирование свободного оборота данных в условиях развития инновационной экономики.

4. Принятие специального закона (Федерального закона «Об экономике данных»).

§ 2.2. Зарубежный опыт информационно-правового обеспечения цифровой экономики

В современных реалиях органы власти и государство, в целом, должны строить свою работу с учетом ожиданий общественности, чтобы успешно работать и иметь возможность реагировать на постоянно меняющиеся условия и запросы граждан. Те государства, которые делают стратегические инвестиции в развитие цифровой «единой среды», намного чаще оправдывают ожидания своих граждан в сфере предоставления им государственных услуг, достигают своих национальных целей и получают выгоду от цифровых инвестиций.

Так, Германия, будучи лидером производства в Европе, первой сделала «Индустрию 4.0» целью специальной правительственной программы, с акцентом на совместную работу бизнеса и государства ради сохранения и увеличения конкурентного преимущества своих производителей[249]. То есть можно сказать, что Германия сделала стратегические инвестиции в развитие модели государственно-частного партнерства (далее – ГЧП), опираясь на цифровое развитие госсектора.

[249] Юдина М.А. Индустрия 4.0: перспективы и вызовы для общества // Государственное управление. Электронный вестник. 2017. № 60. С. 197-215.

Концепция «Индустрия 4.0» часто взаимозаменяемо используется с понятием четвертой промышленной революции. Для нее характерным является: большая автоматизация (по сравнению с третьей промышленной революцией), соединение физического и цифрового мира с помощью киберфизических систем, которые поддерживаются IoT (Интернет вещей)[250].

Конечно, изначально правительство Германии ориентировалось на инновационное развитие промышленности, используя данную концепцию в специальных правительственных программах. Однако с экспоненциальным распространением различных цифровых технологий во всевозможные сферы жизни общества, диктующих человеку новый бытовой порядок, власти Германии приняли решение использовать потенциал и возможности «цифрового мира» и в сфере государственного управления.

Естественно, реализация такой масштабной Стратегии не обходится без сложностей. Но, опуская такие тривиальные проблемы цифровизации как отсутствие единых стандартов, обеспокоенность относительно сетевой безопасности и цифровое неравенство между разными поколениями, Германия имеет и свои специфические проблемы. Например, имеет место быть разный уровень цифровизации между восточными и западными землями ФРГ, а также между коренным населением и мигрантами. Кроме того, Правительство ФРГ активно развивает международное сотрудничество, чтобы с помощью развития цифровой экономики использовать кумулятивный эффект объединенных усилий в сфере цифровой трансформации.

В принципе, в сфере цифровизации государственного управления существенный прогресс наблюдается во всех странах Европейского Союза в плане проводимой политики, что «готовит почву» для внедрения цифровых инноваций.

---

[250] Храмов А.Д., Раева М.О., Петров П.С. Индустрия 4.0 и Качество 4.0: Особенности влияния на современную промышленность // Основные тенденции развития инновационного предпринимательства в реальном секторе экономики в эпоху цифровизации: вызовы и возможности. М.: ИП Сафронов Р. А., 2021.

К примеру, Совет ЕС 1 октября 2021 года поддержал проект Data Governance Act (DGA) – закон об управлении данными[251]. Цель DGA Совет ЕС определяет как «создание надежных механизмов, позволяющих использовать повторно определенные категории защищенных данных». Упоминается также о «росте доверия к услугам передаче данных» и «поощрении альтруизма в отношении данных по всему ЕС», но главная цель – ввести данные, которые защищены законом, в экономический оборот[252].

DGA, по своей сути, является стратегией, призванной создать механизм для обеспечения вторичного использования данных (то есть для целей, не заявленных при сборе данных), которые являются предметом чьих-либо прав и защищены законом (например, интеллектуальная собственность или персональные данные) при условии сохранения их конфиденциальности. Но главная, на взгляд диссертанта, особенность проекта в том, что он создает фундамент для появления новой бизнес-модели – так называемых посреднических сервисов обмена данными (data intermediation services) – которые призваны обеспечивать безопасное пространство для обмена данными без нарушения прав граждан и юридических лиц. Однако для претворения DGA в жизнь необходимо решить ряд вопросов:

– во-первых, распределить сферы юрисдикции между DGA и GDPR (General Data Protection Regulation)[253], а именно: необходимо четко определить, кто несет ответственность и осуществляет гарантии защиты персональных данных на каждом этапе их использования, в соответствии с DGA;

– во-вторых, необходимо определить соотношение полномочий и ответственности надзорных органов при перемещении персональных данных между государствами-членами ЕС.

---

[251] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 may 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). [Электронный ресурс]. URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng (дата обращения: 22.04.2024 г.).

[252] О проекте европейского закона об управлении данными – Data Governance Act. URL: https://d-russia.ru/o-proekte-evropejskogo-zakona-ob-upravlenii-dannymi-data-governance-act.html (дата обращения: 22.04.2024).

[253] Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation / GDPR) // Текст перевода официально опубликован не был; текст Регламента на английской языке опубликован в официальном Журнале, № L 119. 04.05.2016. С. 1-88.

В принципе, данные вопросы не представляются большой проблемой, так что в ближайшее время стоит ожидать прорывов в области цифровой трансформации государственного управления ввиду введения DGA, что может помочь в решении ряда проблем, связанных с цифровизацией государственного управления, поскольку DGA представляет собой набор правил и стандартов по управлению данными, который направлен на их защиту и гарантирование их конфиденциальности, целостности и доступности. Кроме того, это обеспечит более эффективное управление данными и повысит их качество, что улучшит принятие решений и повысит эффективность работы государственных служб, а это, в свою очередь, уже дает начало немного другой концепции – «цифровому правительству».

Считается, что США стали первой страной, официально закрепившей успех в области цифровой трансформации государственного управления, поскольку именно здесь в 2013 году было объявлено о завершении важной цифровой инициативы. Модель «цифрового правительства» в США включает три ключевых уровня:

– информационный уровень, который лежит в основе последующей обработки информации, получаемой из разнообразных источников;

– платформенный уровень, состоящий из всех цифровых систем и аппаратных средств, задействованных для контроля над потоками информации на информационном уровне. Он предоставляет техническую основу для эффективного взаимодействия с данными;

– представительский уровень, функционирует как мост между информационным и технологическим уровнями, формируя интегрированную систему[254].

Структура концепции цифрового управления разграничивает процедуры превращения данных в информацию и последующую передачу этой информации

[254] Digital Government. Building a 21st Century Platform to Better Serve the American People. [Электронный ресурс]: [сайт]. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html. (дата обращения: 02.03.2025).

пользователям, обеспечивая тем самым возможность многократного использования однажды созданного контента по-разному. Благодаря этой модели удалось достичь ряда результатов:

– обеспечен доступ к публичной государственной информации для всех желающих, в любое время и с любого устройства, что сделало информацию более доступной для граждан;

– данные, предоставленные в рамках открытого правительства и доступные в простых форматах, стали стимулировать инновации и экономический рост;

– цифровые технологии способствовали повышению прозрачности, эффективности и результативности работы правительства[255].

Тем не менее, хоть цифровая модель государственного управления США и обладает рядом преимуществ, она также сталкивается с определенными недостатками. Ключевой проблемой является отсутствие непосредственного общения с населением. Это может привести к ситуациям, когда люди могут быть исключены из программ социальной помощи на основании технических или алгоритмических параметров – например, если они не имеют номера социального страхования или не предоставили требуемую налоговую документацию. Такой подход игнорирует комплексность жизненных обстоятельств тех индивидуумов, которые, по каким-то причинам, не удовлетворяют этим формальным требованиям. В результате возникает опасность того, что система цифрового управления может задержать или незаконно отказать в предоставлении социальной поддержки нуждающимся гражданам.

Калифорнийский Закон о защите данных потребителей, принятый в 2018 г. (The California Consumer Privacy Act of 2018)[256] и вступивший в силу с 1 января 2020 г., затрагивает только те компании, которые расположены непосредственно в

---

[255] Дрожжинов В.И., Куприяновский В.П., Евтушенко С.Н., Намиот Д.Е. Стратегический подход к формированию цифрового правительства США // International Journal of Open Information Technologies. 2017. № 4. С. 29-54.

[256] The California Consumer Privacy Act of 2018. [Электронный ресурс]. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (дата обращения: 23.04.2024).

штате, как, например, Google и Facebook[257]. Вместе с тем можно прогнозировать, что в будущем подобные законы появятся и в других штатах.

Другая страна, славящаяся своими достижениями в цифровых технологиях, Япония, активно продвигает инициативы цифрового правительства, такие как: проведение различных административных процедур в онлайн-режиме. Так, в 2018 году Министерство сельского хозяйства, лесного хозяйства и рыболовной промышленности Японии (далее - MAFF) создало единую платформу приложений для подачи заявок (известную как eMAFF), которая позволяет подавать заявки на основе законов и нормативных актов, находящихся под его юрисдикцией, а также заявки на субсидии и гранты в режиме онлайн. Всего японцы перевели в онлайн около 1300 процедур[258].

Помимо очевидных преимуществ различного рода электронного документооборота, такая система позволяет не заботиться о проставлении штампов на документах, поскольку использует идентификатор, выданный Общей корпоративной платформой аутентификации (G Biz ID), установленной Министерством экономики, торговли и промышленности.

Естественно, японское правительство столкнулось с некоторыми проблемами при внедрении eMAFF: сельское, лесное и рыбное хозяйства не являются растущими или развивающимися отраслями, поскольку в них происходит постепенное старение кадров и, как следствие, развивается нехватка рабочей силы и необходимость в повышении квалификации кадров.

Вышеуказанные проблемы могут привести к тому, что данные, хранящиеся в компаниях, будут разрознены, управление ими будет затруднено, а сами данные не будут использованы полностью[259]. Зная о проблемах, Министерство предлагает образовательные программы для повышения грамотности сотрудников в отношении цифровых данных, управляет организацией оцифровки данных,

---

[257] Принадлежит компании Meta, признанной экстремисткой и запрещенной на территории Российской Федерации.

[258] Единая служба приложений Министерства сельского хозяйства, лесного хозяйства и рыболовной промышленности Японии (eMAFF) (пер. с яп.). URL: https://www.maff.go.jp/j/kanbo/dx/emaff.html (дата обращения: 02.03.2025).

[259] Японский консорциум по управлению данными (JDMC) принимает решение о вручении наград MAFF за управление данными в 2022 году (пер. с яп.). URL: https://re-how.net/all/1744762/l (дата обращения: 02.03.2025).

хранящихся в каждой компании отрасли, и способствует максимизации полезного использования данных, доступных внутри и за пределами каждой компании. Для притока же рабочей силы Министерству приходится разрабатывать стратегии привлечения кадров.

Китай, как экономический центр Азии, активно продвигает технологии нового поколения с целью обогнать США в технологической гонке. Уже в 2020 году страна начала активно разрабатывать и внедрять такие инновации, как 5G, искусственный интеллект, беспилотные автомобили и другие передовые технологии. В рамках реализации концепции электронного управления особенно акцентируется внимание на его прогрессировании, соразмерном с демографическими показателями, что предопределяет обширность и высокую степень сложности данных начинаний.

Китайские власти активно занимаются разработкой амбициозного проекта, который предусматривает создание «единой карты». Этот инструмент будет не только решать текущие задачи, связанные с трудоустройством и страхованием, но и обеспечивать слияние государственных услуг. Он позволит упростить процедуры приобретения медикаментов, управления государственными субсидиями и выполнять множество других функций. Проект направлен на значительное улучшение качества предоставляемых государственных сервисов[260].

«Единая карта» будет разработана с использованием блокчейн-технологий, что гарантирует надежную защиту и открытость информации. В то же время, существующий портал государственных услуг применит инструменты Big Data для объединения и анализа информации. Несмотря на то, что сама технология «больших данных» уже стала привычной, китайские власти планируют расширить ее функциональные возможности, включая, помимо традиционного анализа больших объемов данных, также анализ тенденций, что позволит улучшить прогнозирование и принятие решений на уровне государственного управления. Несомненно, специфической особенностью Китая является численность его

[260] Джан Л., Чен С. Цифровая экономика Китая: возможности и риски // Вестник международных организаций: образование, наука, новая экономика. 2019. Т. 14. № 2. С. 283.

населения: «приспособить» все население КНР к данным новшествам – задача сложная, на выполнение которой уйдет немало лет. Однако, вероятно, основные трудности придутся лишь на меньшую часть населения – ту, что живет не в городах, а на севере и западе Китая, в сельской местности.

Кроме того, законом КНР «Об электронной коммерции», вступившим в силу с 1 января 2019 г., потребителям предоставляется защита от ложных отзывов о продукции, нормативный правовой акт формирует основу для борьбы с контрафактной продукцией и систематизацией деятельности участников рынка[261]. К таковым отнесены отзывы, написанные не только нанятыми сотрудниками, но и другими клиентами в случае получения от фирмы какого-либо денежного вознаграждения.

Примером весьма успешной цифровой инновации является платформа финансовых цифровых услуг Etimad, запущенная Министерством финансов Саудовской Аравии в апреле 2021 г. Она предоставляет множество услуг государственным учреждениям, целью которых является упрощение операционных процедур и документирования финансовых операций коммерческих организаций с государственным сектором, а также предоставление инструментов для объективной оценки уровня обслуживания, что направлено на повышение эффективности обслуживания[262]. Можно выделить следующие основные результаты, достигнутые благодаря внедрению Etimad:

– повышение прозрачности проведения государственных тендеров;

– упрощение и стандартизация операционных процедур;

– повышение эффективности расходов государственных органов;

– увеличение участия малого и среднего бизнеса в экономическом развитии страны.

Основной проблемой, с которой столкнулась Саудовская Аравия при внедрении данной платформы, является перенос и интеграция актуальных данных

---

[261] 中华人民共和国电子商务法 № 7 (Закон КНР «Об электронной коммерции» от 31.08.2018). URL: http://www.mofcom.gov.cn/article/zt_dzswf/deptReport/201811/20181102808398.shtml (дата обращения: 23.04.2024).

[262] Etimad – платформа финансовых цифровых услуг (пер. с араб.). URL: https://portal.etimad.sa/. (дата обращения: 02.03.2025).

в платформу, поскольку на тот момент со стороны Саудовской Аравии наблюдались значительные задержки платежей по контрактам, выполненным США для саудовских государственных и частных организаций, что создавало большую разрозненность данных[263].

Другая страна – Великобритания – отличающаяся особой строгостью и традиционностью, уже с 2004 года имеет сайт электронного правительства, славящийся своим минимализмом и функциональностью, который постоянно совершенствуется в области кибербезопасности.

В 2018 году правительство Великобритании приняло решение адаптировать шпили церквей по всей стране для создания цифровых коммуникационных каналов, включая установку WiFi-передатчиков и антенн. Это предоставило возможность жителям сельских районов получить доступ к «Интернету», что значительно упростило их связь с государственными службами, предоставило возможность для общения с друзьями и родственниками, развития бизнеса, образования и других аспектов жизни.

Наиболее интересным проектом по цифровой трансформации государственного управления является «Biometrics Strategy», в рамках которого в 2018-ом году была создана единая база биометрических данных граждан Великобритании. С созданием данной базы значительно упростилась работа британского МВД по розыску преступников и ускорился рабочий процесс сотрудников пограничной службы, поскольку в эту базу входят ДНК, отпечатки пальцев и фотографии лиц[264]. В будущем список планируется пополнять и другими данными, например образцами голоса граждан. Такая информация преимущественно доступна МВД Великобритании, полиции, миграционным службам и работникам паспортного контроля в аэропортах и пограничных зонах.

Несмотря на такие успехи, британцы, конечно же, столкнулись с классическими трудностями: такими, как вопросы информационной безопасности,

---

[263] Saudi Arabia market challenges - Official Website of the International Trade Administration. URL: https://www.trade.gov/knowledge-product/saudi-arabia-market-challenges/ (дата обращения: 02.03.2025).

[264] Лебедева Е.А., Сладкова А.В. О цифровых технологиях контроля в государственном управлении в зарубежных странах // Административное право и процесс. 2020. № 7. С. 83-88.

низкая квалификация сотрудников государственного сектора на начальном этапе и высокие издержки. Однако, применительно к Великобритании, издержки оказались высоки не столько из-за стоимости всего высокотехнологического, сколько из-за того, что цифровая трансформация государственного управления там началась еще в 2004 году с сайта электронного правительства, для которого поначалу, в силу отсутствия острой необходимости, обновления и актуализация технологий сбора данных шли медленными темпами, из-за чего впоследствии пришлось наращивать этот темп в разы быстрее, чем в других странах. Конечно, было бы дешевле, если бы цифровое правительство появилось позже, но сразу с более совершенными технологиями, но тогда бы имел место другой сдерживающий фактор: неподготовленность населения.

В 1999 г. около 47 штатов США приняли Единообразный закон об электронных сделках (UETA)[265]. Важно отметить, что это предоставляет человеку, который использует технологию блокчейн, возможность защищать информацию и иметь те же права собственности, что и лицо, которое использует традиционные средства.

Представляется обоснованным выделить как одно из успешных решений метод поэтапного правового внедрения инноваций, реализуемый в Китае. Такой подход заключается в установлении правовых экспериментов: вначале новые нормы апробируются в ограниченных сферах или отдельных регионах, после чего, на основе тщательно проведенного анализа результатов, мониторинга и экспертной оценки, меры, показавшие свою эффективность, либо тиражируются на более широкий круг отношений, либо закрепляются в форме общегосударственного законодательства. В качестве яркого примера можно привести эволюцию нормотворчества, осуществленную при подготовке и утверждении Закона КНР «Об электронной коммерции», когда успешные элементы были перенесены из пилотных практик в закон на национальном уровне[266].

---

[265] Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / М.О. Дьяконова, А.А. Ефремов, О.А. Зайцев и др.; под ред. И.И. Кучерова, С.А. Синицына. Москва: ИЗиСП, НОРМА, 2022. 376 с.

[266] Алексеенко А.П. Регулирование деятельности электронных платформ по Закону КНР «Об электронной коммерции» // Юрист. 2020. № 7. С. 62-68.

ГЛАВА 3. ОСОБЕННОСТИ ИНФОРМАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ В ОТДЕЛЬНЫХ СФЕРАХ ЦИФРОВОЙ ЭКОНОМИКИ

§ 3.1. Информационно-правовое обеспечение в сфере цифровых финансовых активов

Появление цифровых финансовых активов является результатом растущего спроса на глобальные изменения в информационной, правовой и экономической сферах, которые возникают в результате внедрения современных информационных технологий в различные сферы нашей жизни.

Цифровая экономика, основанная на использовании информационных технологий и цифровых платформ, привела к необходимости внесения изменений в нормативные правовые акты, чтобы учесть новые правила и рекомендации, представленные Центральным банком Российской Федерации. Эти изменения направлены на создание регулирующей среды, которая бы обеспечивала безопасность и стабильность в использовании цифровых финансовых активов.

Кроме того, появление цифровых финансовых активов привело к возникновению новых субъектов информационной инфраструктуры, таких как операторы и пользователи информационных систем. Операторы информационных систем обеспечивают функционирование и управление цифровыми финансовыми активами, а пользователи являются активными участниками, осуществляющими операции с этими активами.

В целом появление цифровых финансовых активов является результатом глобальных изменений, связанных с внедрением информационных технологий и строительством цифровой экономики, что требует внесения изменений в нормативные правовые акты[267].

Развитие цифровых технологий и потребности в правовом регулировании операций с ними привели к появлению информационных правоотношений в сфере цифровых финансовых активов с целью установления общих стандартов и

[267] Рустамов П.А. Перспективы правового регулирования цифровых валют в Российской Федерации // International Law Journal. 2022. № 7. С. 144.

принципов, которые способствуют сотрудничеству и координации в рассматриваемой сфере.

Цифровые активы являются электронным воплощением ценности и могут применяться для осуществления разнообразных операций, таких как покупка, продажа или обмен. Эти активы обращаются при помощи блокчейн-технологии, которая гарантирует надежность и прозрачность совершаемых транзакций.

В настоящее время некоторые страны стали особенно активными в развитии и принятии цифровых активов и блокчейн-технологий, а также являются лидерами и первопроходцами в части информационно-правового регулирования данной отрасли. Регулирование правовых взаимоотношений в секторе управления цифровыми финансовыми активами осуществляется, чаще всего, посредством использования целого ряда правовых документов, а не через единственный специализированный законодательный акт. США выделяются как одна из лидирующих держав в сфере создания и нормативного управления цифровыми финансовыми активами, что включает в себя принятие соответствующего законодательства и формирование регулирующих органов для контроля над оборотом и использованием этих активов[268]. Согласно Закону о ценных бумагах (Securities Act), выпуск и обращение цифровых активов могут быть квалифицировано наравне с ценными бумагами, оборот ЦФА регулируется Законом о ценных бумагах и биржах (Securities Exchange Act), который устанавливает требования к регистрации и деятельности цифровых активов, которые являются ценными бумагами, на биржах и другими нормативными правовыми актами.

Швейцария также заслужила репутацию благожелательной к цифровой финансовой среде, способствуя возникновению и росту обширного количества блокчейн-инициатив и предприятий, а равно разрабатывая специализированные законодательные и регуляторные механизмы, в частности, в Швейцарии возможна

[268] Securities Act (1933) as Amended Through P.L. 115–174, Enacted May 24, 2018. URL: https://www.fsc.go.kr/comm/getFile?srvcId=BBSTY1&upperNo=27272&fileTy=ATTACH&fileNo=2 (дата обращения: 07.07.2025).; Securities Exchange Act (1934) as Amended Through P.L. 112–158, Approved 10 August 2012. URL: https://www.govinfo.gov/content/pkg/COMPS-1885/pdf/COMPS-1885.pdf (дата обращения: 07.07.2025).

эмиссия акций компаний с ограниченной ответственностью в рамках частной децентрализованной системы[269].

В последние годы все больше стран инкорпорируют ЦФА в свои финансовые системы, например Германия[270], Заморская территория Великобритания - Кайманы[271] активно внедряют и регулируют ЦФА[272]. Распространение и принятие цифровых финансовых активов продолжают расти по всему миру, и каждая страна разрабатывает свои собственные подходы к их регулированию и использованию.

Цифровые единицы обладают основными характеристиками:

1. Используются в качестве платежного средства;
2. Применяются для торговых транзакций;
3. Могут выступать в роли инструмента для накопления и сохранения капитала;
4. Исполняют функцию учета и расчетов.

Цена на цифровые валюты, несмотря на их инновационный характер, определяется балансом между спросом и предложением участников сети.

Цифровая валюта базируется на математических принципах и применяет криптографические технологии. Для ее обращения необходимо наличие информационно-телекоммуникационной сети.

Таким образом, цифровые валюты и токены являются разновидностями цифровых активов, но имеют различные функции и характеристики. Цифровые валюты обычно используются в качестве средства обмена и хранения стоимости, в то время как токены могут иметь более широкий спектр использования и представлять различные права и возможности.

---

[269] Federal Act on the Amendment of the Swiss Civil Code (Part Five: the Code of Obligations) of 30 March 1911 (Federal Act) (1911) Government of the Swiss Confederation.

[270] Electronic Securities Act (eWpG) (Law of 3 June) (2021). URL: https://www.loc.gov/item/global-legal-monitor/2021-06-29/germany-electronic-securities-act-enters-into-force/ (дата обращения: 07.07.2025).

[271] Virtual asset (service providers) Act (2022 Revision) Supplement No. 6 published with Legislation Gazette No. 7 dated 31st January, 2022. URL: https://legislation.gov.ky/cms/images/LEGISLATION/PRINCIPAL/2020/2020-0014/VirtualAssetServiceProvidersAct_2022%20Revision.pdf (дата обращения: 07.07.2025).

[272] Практика по регулирования рассматриваемых отношений отличается. Некоторые страны создают новое законодательство (как показано выше в работе), некоторые вносят изменения в действующей и распространяют знакомые подходы на новые отношения.

Криптоактивы разделяются на несколько ключевых категорий в зависимости от их природы и функций: токены для инвестирования, утилитарные токены, цифровые валюты, биржевые монеты, токены приложений и альтернативные монеты.

Допускается проведение классификацию цифровых финансовых активов, опираясь на набор взаимоисключающих характеристик и следуя установленным принципам. В этом контексте можно идентифицировать по различным категориям: основные криптоактивы, утилитарные токены, инвестиционные токены, товары в криптовиде, токены приложений и стейблкоины. Активы, группированные в каждую из категорий, обладают общими свойствами. Они похожи по функционалу, по реакции на рыночную конъюнктуру, схожи моделями оценки. У классов активов могут быть общие модели оценки, но разные цели и функции[273].

В целом цифровые финансовые активы могут быть классифицированы по различным критериям, представленным в таблице 2.

Таблица 2 – Классификации цифровых финансовых активов

Основание классификации	Виды цифровых финансовых активов
1. По способу выпуска	– Инициальное предложение монет (ICO). Процесс, при котором компания или проект выпускает свои собственные токены и продает их инвесторам для привлечения финансирования. – Секьюрити токены. Токены, которые представляют ценные бумаги, такие как акции, облигации. Секьюрити токены обычно регулируются соответствующими финансовыми органами и подчиняются правилам и нормативам, которые применяются к традиционным финансовым инструментам. – Утилитарные токены. Токены, которые предоставляют доступ к определенным услугам или продуктам, предлагаемым на блокчейн-платформе. Утилитарные токены не являются ценными бумагами и обычно не регулируются как финансовые инструменты.
2. По уровню децентрализации	– Централизованные активы. Активы, которые контролируются и управляются центральными органами или компаниями. Примером может служить цифровая валюта, выпущенная центральным банком. – Децентрализованные активы. Активы, которые не имеют центрального контроля и управления.

[273] Классификация криптоактивов: от служебных токенов до платформ // Криптовалюта. URL: https://cryptocurrency.tech/klassifikatsiya-kriptoaktivov-ot-sluzhebnyh-tokenov-do-platform/ (дата обращения: 02.03.2025).

Цифровые активы представляют собой сравнительно новую сферу в контексте информационного права и, как следствие, ставят перед законодателем задачу создания специализированного правового регулирования. Важным аспектом такого регулирования является разработка правил и стандартов, которые призваны не только защищать интересы и права владельцев и пользователей цифровых активов, но и обеспечивать стабильность и безопасность этих активов в рамках информационного пространства.

Особенностью цифровых финансовых активов является их функционирование на базе блокчейн-технологий. Эти технологии позволяют проводить транзакции напрямую между участниками сети, исключая традиционных посредников, таких как банковские и финансовые институты, а также государственные организации. Такой подход к транзактированию кардинально отличается от механизма работы традиционных финансовых активов, где централизованные посредники необходимы для проведения и подтверждения финансовых операций.

Технология блокчейн существенно повышает открытость операций с цифровыми финансовыми активами благодаря ведению общего распределенного реестра, в котором фиксируются все транзакции. Данный реестр находится в свободном доступе для каждого участника сети, что облегчает процесс контроля и проверки совершаемых операций.

Такая архитектура способствует укреплению доверия между участниками системы и снижает вероятность мошеннических действий. Вместе с тем вопросы юридического статуса и правового регулирования цифровых финансовых активов находятся в стадии формирования и по-разному решаются в различных национальных правопорядках[274].

Рассмотрим основных субъектов информационно-правовых отношений в сфере цифровых финансовых активов.

---

[274] Данный тезис подтверждается фактом формирования судебной практики по исследуемому вопросу - Решение Арбитражного суда Удмуртской области от 05.11.2024 по делу № А71-18227/2024. URL: https://kad.arbitr.ru/Card/22beb57b-a063-4006-b8a5-4ab83d0acbcc. По материалам дела участники рынка ЦФА подали иск о взыскании залога в рамках сделки по выпуску ЦФА. Иск удовлетворен полностью.

В контексте взаимодействий с цифровыми финансовыми активами государство несет ключевую ответственность за установление правил и стандартов через принятие законодательных актов и обеспечивает надзор за их соблюдением. Это происходит благодаря работе законодательных структур, которые создают правовую базу для цифровых активов, а также через действия исполнительной власти, которая обеспечивает выполнение установленных законом предписаний. Судебные инстанции также играют роль в этой системе, рассматривая споры и нарушения в рамках данной сферы. Кроме того, исполнительные органы могут проводить аудиты и проверки для обеспечения прозрачности и надежности в сфере цифровых финансовых активов.

Государство осуществляют контроль за деятельностью компаний, занимающихся цифровыми финансовыми активами, и обеспечивают соблюдение правил и требований, установленных законодательством, могут выдавать лицензии, проводить проверки и расследования.

Следовательно, в контексте цифровых финансовых активов, государство выступает ключевым игроком в регулятивных и надзорных процессах данного сектора, гарантируя законодательную базу, прозрачные условия работы, безопасность и защиту прав потребителей.

Кредитные организации в качестве субъектов правоотношений в сфере цифровых финансовых активов предоставляют услуги по их обмену. Кроме того, кредитные организации оказывают услуги по хранению цифровых активов и могут выполнять функцию посредника в соответствующих сделках.

Пользователи цифровых финансовых активов как субъекты информационных правоотношений в сфере цифровых финансовых активов могут быть как индивидуальными инвесторами, так и представителями хозяйствующих субъектов. Данный вид субъектов информационных правоотношений осуществляют покупку и продажу (расчеты) цифровых финансовых активов, а также реализовывают функции инвестирования и тому подобное.

Технологические платформы, особенно интернет-платформы и торговые площадки, предоставляют среду для коммерческой активности и обмена в сфере

цифровых финансовых активов, выступая в качестве элементов информационных отношений. Они дают участникам доступ к рынку и гарантируют проведение транзакций. В общем контексте, данные платформы играют ключевую роль в секторе цифровых финансов, обеспечивая необходимую инфраструктуру и сервисы для пользователей при этом придерживаясь законодательных стандартов и требований.

Разработчики и IT специалисты – это лица или организации, которые заняты созданием и поддержанием технического оснащения для работы с цифровыми финансами. В эту деятельность входит разработка блокчейнов, применение методов криптографии и прочие направления.

Интеграция цифровых активов – это процесс объединения различных цифровых ресурсов и активов в рамках единой системы или платформы, одной из основных целей такой интеграции является увеличение эффективности и оптимизация бизнес-процессов. Путем объединения различных активов в одну систему, компании могут улучшить координацию работы, сократить время на выполнение задач и повысить качество предоставляемых услуг. Интеграция цифровых активов также позволяет улучшить взаимодействие между различными системами и устройствами. Например, благодаря интеграции можно обеспечить совместимость между различными программными продуктами, что упрощает передачу данных и обмен информацией.

Одной из популярных форм интеграции цифровых активов является API-интеграция. API (Application Programming Interface) – это набор инструментов и протоколов, которые позволяют различным приложениям взаимодействовать друг с другом. Благодаря API-интеграции, различные системы могут обмениваться данными и использовать функциональность друг друга. Интеграция цифровых активов имеет множество применений в различных сферах бизнеса. Например, в сфере электронной коммерции интеграция позволяет объединить различные онлайн-магазины, платежные системы и логистические сервисы для обеспечения более удобного и эффективного процесса покупки и доставки товаров. Также интеграция цифровых активов актуальна в области управления предприятием, где

объединение различных систем позволяет автоматизировать бизнес-процессы, управлять ресурсами и оперативно получать аналитическую информацию.

Одним из примеров интеграции цифровых финансовых активов в России является ПАО «ГМК «Норильский никель» (Норникель) – крупнейшая металлургическая и горнодобывающая компания в России и мировой лидер в производстве никеля и палладия. В рамках своей цифровой трансформации Норникель использует различные инновационные решения и технологии, такие как интернет вещей (IoT), искусственный интеллект (ИИ) и аналитика данных, которые применяются для мониторинга и управления производственными процессами, повышения эффективности и безопасности работы, а также для оптимизации использования ресурсов. ПАО «ГМК «Норильский никель» (Норникель), в рамках стимулирующей программы, предоставляет работникам цифровые активы, приравненные по стоимости к акциям компании[275].

Информационные правоотношения в сфере цифровых финансовых активов регулируются достаточно широким перечнем нормативных правовых актов. Принятый в 2006 году Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ устанавливает общие принципы и требования к обработке информации, определяет правовые основы для обеспечения безопасности информации, включая защиту от несанкционированного доступа, модификации и распространения данных, что особенно важно в контексте цифровых финансовых активов, где безопасность и надежность хранения и передачи данных являются критическими, и так далее[276].

Для развития ряда положений данного нормативного правового акта и в связи со сложившейся потребностью в специализированном нормативном правовом акте для регулирования электронной подписи в 2011 году был принят одноименный Федеральный закон № 63-ФЗ[277]. Также в 2011 году был принят Федеральный закон

---

[275] «Цифровые активы» выпустили первые токены для участников корпоративной программы «Норникеля» URL: https://nornickel.ru/news-and-media/press-releases-and-news/tsifrovye-aktivy-vypustili-pervye-tokeny-dlya-uchastnikov-korporativnoy-programmy-nornikelya/ (дата обращения: 02.03.2025).

[276] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

[277] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Российская газета.08.04.2011. № 75.

от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе»[278]. В контексте развития цифровых финансовых активов, Закон № 161-ФЗ определяет электронные денежные средства как специальный вид денежных средств, используемых в электронной форме, устанавливает правила и требования к эмитентам электронных денежных средств, а также определяет права и обязанности пользователей таких средств, устанавливает требования к защите персональных данных и обеспечению безопасности платежных операций и определяет правила и требования к платежным системам, включая системы электронных платежей, устанавливает процедуры лицензирования и надзора за платежными системами, что способствует развитию надежных и эффективных платежных инструментов, включая цифровые финансовые активы.

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» прямо не затрагивает вопросы регулирования цифровых финансовых активов, однако он определяет стратегическую цель обеспечения информационной безопасности в области науки, технологий и образования[279]. Цель состоит в стимулировании передового и интенсивного прогресса в сфере информационной безопасности, информационно-технологической отрасли и электронной индустрии. Препятствием для достижения этой цели является неадекватная поддержка для ускорения развития систем защиты информации, а также IT-сектора и электронного производства в общем. Это во многом обусловлено неурегулированностью соответствующей правовой базы, которая не отвечает текущим требованиям и вызовам, связанным с развитием цифровых технологий.

К приоритетным задачам в сфере информационной безопасности по научной, технологической и образовательной деятельности относятся:

---

[278] Федеральный закон от 27.06. 2011 года № 161-ФЗ «О национальной платежной системе» // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.

[279] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7077.

а) повышение конкурентных преимуществ российских информационных технологий и укрепление научно-технической базы для гарантирования информационной безопасности;

б) разработка и апробация IT-систем, интегрированных с механизмами устойчивости к различным формам атак;

в) выполнение исследований и экспериментальное проектирование с целью создания новаторских информационных технологий и методик защиты информации;

г) формирование профессионального состава специалистов в домене защиты информации и использования IT-инструментов;

д) обеспечение личной неприкосновенности граждан в отношении информационных рисков, включая развитие навыков личного обеспечения информационной безопасности[280].

Далее был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ[281]. Этот нормативный правовой акт устанавливает требования к операторам критической информационной инфраструктуры, включая операторов цифровых финансовых активов, и регулирует их обязанности по обеспечению безопасности информационных систем и сетей. Он также описывает правила взаимодействия операторов с государственными органами в случае возникновения угроз безопасности. Закон включает меры государственной поддержки и стимулирования безопасности критической информационной инфраструктуры, включая сферу цифровых финансовых активов. Он определяет правила предоставления государственных услуг и финансовой поддержки, а также механизмы координации деятельности по обеспечению безопасности в данной области.

---

[280] Там же.

[281] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Российская газета. 31.07.2017. № 167.

В 2019 году была принята Национальная программа «Цифровая экономика Российской Федерации», цель которой заключается в создании и развитии полноценной экосистемы цифровой экономики[282].

Центральное место в рамках обозначенной программы занимает стимулирование и развитие рынка цифровых финансовых активов, с акцентом на совершенствование технологических инструментов и создание условий для эффективного внедрения цифровых финансовых решений. В контексте программы предвидится разработка нового комплекса законодательства и формирование регулятивных механизмов, которые обозначат путь для инновационного развития в данной области.

Правовое регулирований цифровых финансовых активов должно быть поэтапным, учитывая характер исследуемых объектов необходимо коллективная работа по гармонизации международного законодательства в данной сфере[283].

Программа также намечает стратегию построения инфраструктуры, необходимой для поддержания циркуляции и эффективного использования цифровых финансовых активов. Это включает в себя создание и развитие цифровых платформ и сервисов, обеспечивающих удобное, безопасное и надежное хранение, трансфер и обмен данными активами. Такая инфраструктура служит не только удобству пользователей, но и повышает общую безопасность и стабильность финансового оборота в цифровой экосистеме.

Стоит отметить, что в 2025 году стартовал национальный проект «Экономика данных и цифровая трансформация государства», направленный на развитие экономики на основе данных, которые генерируются в цифровых системах – как бизнеса, так и государства, который станет продолжением завершающегося Национальной программы «Цифровая экономика Российской Федерации»[284].

---

[282] Национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4. 06. 2019 г. № 7. URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fwww.google.com%2f#section-docs.

[283] Морозов А.В. Регулирование рынка криптовалют (информационно-правовой аспект) // Вестник Московского университета. Серия 26. Государственный аудит. 2019. № 2. С. 15.

[284] Национальный проект «Экономика данных и цифровая трансформация государства». URL: https://xn--80aapampemcchfmo7a3c9ehj.xn--p1ai/new-projects/ekonomika-dannykh/.

Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» является основным в правовом регулировании оборота цифровых финансовых активов[285]. Федеральный закон № 259-ФЗ внес изменения в отдельные законодательные акты, чтобы установить правовые нормы для регулирования оборота цифровых финансовых активов и цифровой валюты, что создает стабильность и прозрачность в сфере цифровых финансовых отношений и способствует их развитию и использованию, а также реализует один из основных принципов национальной программы «Цифровая экономика Российской Федерации» – создание благоприятной среды для развития цифровых финансовых технологий.

Среди преимуществ правового регулирования цифровых финансовых активов несколькими нормативными правовыми актами можно выделить гибкость и адаптивность, а также учет разнообразия. В первом случае наличие нескольких нормативных правовых актов позволяет более гибко реагировать на изменения в технологической среде и развитие новых видов цифровых финансовых активов. Разнообразие учитывается путем принятия различных законодательных мер, которые предусматривают индивидуальные черты и характеристики цифровых финансовых активов. Это включает в себя нормы, регулирующие выпуск, оборот, торговлю и хранение данных активов, что способствует более всестороннему и точному надзору за данной областью.

Также можно выделить и недостатки правового регулирования цифровых финансовых активов несколькими нормативными правовыми актами, как сложность и неоднозначность, перекрывающие положения. Так, наличие нескольких нормативных правовых актов может создавать сложности в понимании и применении правил для участников рынка, а различные акты могут содержать разные требования и стандарты, что может создавать неоднозначность. Кроме того, несколько нормативных правовых актов могут содержать положения, которые

[285] Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

перекрываются или противоречат друг другу, что может создавать путаницу и затруднять применение правил.

Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[286] в целом устанавливает правовые основы для регулирования цифровых финансовых активов в России. Однако есть несколько вопросов, которые в законе можно считать недостаточно регулируемыми:

1. Определение и классификация цифровых финансовых активов. Закон описывает цифровые финансовые активы как цифровые права, но не предоставляет четкого определения или классификации различных типов цифровых активов, что может создавать некоторую неопределенность и затруднять применение закона в практике[287].

2. Регулирование торговли цифровыми финансовыми активами. Закон устанавливает правила для организации и осуществления торговли цифровыми финансовыми активами, но не регулирует все аспекты этой деятельности. Например, не указаны требования к торговым платформам, не установлены правила открытия и закрытия позиций, а также не регулируется вопрос о защите прав и интересов инвесторов.

3. Контроль и надзор за цифровыми финансовыми активами. Закон устанавливает принципы и требования к операторам цифровых финансовых активов, но не предоставляет подробных механизмов контроля и надзора за их деятельностью. Отсутствует четкое определение роли и обязанностей регулирующих органов, а также не установлены механизмы наказания за нарушение правил и нормативов. Часть данных положений содержит Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[288].

---

[286] Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

[287] Рустамов П.А. К вопросу о совершенствовании правового регулирования цифровых финансовых активов в России // Евразийская адвокатура. 2024. № 1 (66). С. 146.

[288] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 31.07.2017. № 167.

4. Международное сотрудничество. Закон не содержит подробных положений о международном сотрудничестве в области цифровых финансовых активов. В условиях глобализации и международной природы цифровых активов, необходимо разработать механизмы сотрудничества с другими странами для обмена информацией, борьбы с мошенничеством и предотвращения легализации доходов от преступной деятельности.

В июле 2023 года Президент РФ подписал два закона о цифровом рубле. Федеральный закон от 24.07.2023 № 339-ФЗ «О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» содержит поправки к ГК РФ[289], а Федеральный закон от 24.07.2023 № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» – масштабные изменения нескольких нормативных правовых актов[290].

Производить расчеты цифровым рублем будут путем его перевода на спецплатформе. Цифровой рубль, как цифровой аналог российской национальной валюты, является цифровым финансовым активом, который функционирует на основе технологии распределенного реестра (блокчейн), имеет свою цифровую форму и может быть использован для осуществления платежей и других финансовых операций в цифровой среде.

Цифровой рубль является цифровой валютой. В соответствии с Законом № 259-ФЗ, цифровая валюта определяется как самостоятельный объект гражданских прав, ограниченный в обороте[291]. Организация выпуска и обращения цифровой валюты, включая цифровой рубль, регулируется федеральными законами. Можно обратить внимание, что часто криптовалюту ошибочно относят к ЦФА и цифровым валютам. Криптовалюта имеет особенности, которые отличают ее от цифровой

---

[289] Федеральный закон от 24.07.2023 № 339-ФЗ «О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» // Российская газета. 31.07.2023. № 167.

[290] Федеральный закон от 24.07.2023 № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета. 31.07.2023. № 167.

[291] Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

валюты. Криптовалюта не контролируется центральным банком или государством. Криптовалюты, такие как Bitcoin или Ethereum, не являются законными платежными средствами и их обращение не регулируется федеральными законами. Таким образом, цифровой рубль является цифровой валютой, которая отличается от криптовалюты своим режимом и регулированием[292].

Согласно ст. 3 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» участниками платформы цифрового рубля являются операторы перевода денег (исключая Центральный банк Российской Федерации) или зарубежные банковские учреждения. Эти организации предоставляют доступ клиентам платформы для осуществления транзакций с использованием цифровых рублей[293]. Участники платформы – кредитные организации, которые вправе переводить деньги, госкорпорация развития «ВЭБ.РФ» и иностранные банки. Пользователи (плательщики и получатели) – физлица, индивидуальные предприниматели и организации.

В сфере цифровых финансовых активов инвестиционные операции могут быть связаны с определенными рисками, такими как волатильность рынка, возможность мошенничества, отсутствие гарантий и так далее. В связи с этим, информирование участников об этих рисках является важным аспектом информационно-правового регулирования. Уведомление о рисках может происходить на различных этапах инвестиционных операций. Например, при предоставлении информации о цифровых финансовых активах перед их приобретением, участники должны быть ясно и полно осведомлены о возможных рисках, связанных с такими операциями, включая предупреждения о волатильности рынка, потере инвестиций, возможности мошенничества и других факторах, которые могут повлиять на результаты инвестиций. Дополнительно уведомление о рисках может быть предоставлено во время самой инвестиционной операции, чтобы участники могли принимать осознанные решения на основе

[292] Также существует судебная практика, которая рассматривает криптовалюты как имущество, в том числе имущественные права: Решение Савеловского районного суда от 09.11.2021 г. № 2-2888/2021; Апелляционное определение от 28.09.2023 по делу № 33-39520/2023 (в суде 1-й инст. № 2-3411/2023) // СПС «Консультант Плюс».

[293] Федеральный закон от 27.06.2011 года № 161-ФЗ «О национальной платежной системе». Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.

полной информации, в том числе предупреждения о возможных последствиях, связанных с определенными типами операций, например, с использованием кредитного плеча или участием в ICO (Initial Coin Offering).

Уведомление о рисках обычно включает информацию о возможных негативных последствиях инвестиций, связанных с конкретными цифровыми финансовыми активами, в том числе предупреждения о потере инвестиций, нестабильности рынка, возможности мошенничества и других рисках, которые могут повлиять на результаты инвестиций. Цель такого уведомления субъектов права об инвестиционных рисках заключается в предоставлении им достаточной информации для принятия осознанных решений, что помогает инвесторам оценить свою готовность к риску и принять обоснованные решения на основе полной информации.

Информирование участников сделки с цифровыми финансовыми активами о возможных рисках, связанных с инвестиционной деятельностью, становится одним из ключевых направлений разработки новых норм в области информационно-правового регулирования. Выделим основные проблемные вопросы, отраженные в данном параграфе. Во-первых, правовая база, обеспечивающая информационную безопасность в секторе цифровых активов, остается недостаточно развитой: стороны зачастую действуют в условиях правовой неопределенности. Наиболее сложные моменты связаны с размытым определением информационно-правового положения цифровых финансовых активов и избыточной склонностью к применению административных или силовых инструментов регулирования государством при надзоре за данным рынком. Во-вторых, отсутствие четко закрепленных международных механизмов взаимодействия негативно сказывается на обеспечении безопасности при трансграничном движении цифровых активов. Наконец, представляется необходимым проводить детальное различение между понятиями цифровых финансовых активов и бездокументарных ценных бумаг с целью предотвращения смещения правового содержания при регулировании этих категорий.

§ 3.2. Информационно-правовое обеспечение отношений по осуществлению сделок в цифровой экономике

В цифровой экономике возникают новые виды взаимодействий между людьми, компаниями и государствами, которые ранее не существовали, эти отношения требуют нового правового регулирования, чтобы обеспечить справедливость и защиту интересов всех сторон. Также цифровая экономика меняет традиционные представления о праве и требует новой парадигмы, которая учитывает особенности и вызовы цифровой среды, правовая доктрина должна быть готова адаптироваться к этой новой парадигме и предсказывать развитие правовой системы в цифровой экономике. Цифровая экономика требует трансформации различных отраслей и правовых институтов, некоторые из которых могут быть адаптированы к новым условиям, в то время как другие могут требовать разработки новых правовых механизмов. Правовая политика должна определить приоритеты и направления развития в этой области.

Смарт-контракты требуют создания самостоятельных правовых категорий для их регулирования. А.И. Савельев рассматривает «умный» контракт как неразделимую совокупность двух элементов: программы для ЭВМ и базы данных[294].

Согласно редакции п. 1 ст. 160 Гражданского кодекса РФ, смарт-контракт приравнивается к документальной форме заключения сделки, выполненной в цифровом формате либо при помощи применения технологических устройств. В своей основе смарт-контракт является программным кодом (программой для вычислительных машин), содержащим предустановленный алгоритм выполнения операций. Эти действия, выполняемые последовательно, соответствуют юридически значимым поступкам, таким как заключение соглашения, присоединение к заранее установленным условиям, последовательное исполнение обязательств, обмен цифровыми активами (токенами) и получение встречного удовлетворения, включая получение криптовалюты или услуг.

---

[294] Савельев А.И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 44.

Многие современные правовые трактовки смарт-контрактов основываются на более узком понимании, связывая их регулирование с нормами договорного права. Здесь смарт-контракт воспринимается как инструмент для автоматизации процедуры создания и реализации договоров гражданского характера, при этом компьютерный код выполняет функции формирования, верификации и осуществления взаимных соглашений участников. Кроме того, смарт-контракт представляется как метод автоматизированного исполнения обязательств по договору, что обеспечивает строгое соответствие условиям стандартных бумажных договоров и тех, которые были заключены в виде электронного документа[295].

А.И. Савельев характеризует «интеллектуальные» контракты как программный код, реализованный на технологии блокчейн, который гарантирует автоматическое и самостоятельное выполнение договора при возникновении предусмотренных ситуаций[296]. К числу отличительных черт смарт-контрактов он относит: невозможность их нарушения; неспособность защищать слабую сторону; автономный характер; а также возможность существования смарт-контрактов, противоречащих публичному порядку[297].

С учетом специфики функционирования технологий на базе распределенного реестра, где записи генерируются как результат работы компьютерной программы, управляемой человеком либо автоматически исполняемой прописанным алгоритмом, данные объекты, будучи нематериальными по своей природе, обладают экономической ценностью. Это позволяет рассматривать такие объекты как «иное имущество», что может стать основой для их правового регулирования.

Применение европейской доктрины sui generis, которая признает особую имущественную ценность новых цифровых объектов, представляется более подходящим, чем использование традиционного подхода стран общего права, который делит имущество на недвижимость, вещи (chose in possession) и права (chose in action), независимо от формы существования объекта. Такой подход

---

[295] John Stark. How Close Are Smart Contracts to Impacting Real-World Law? COINDESK (Apr. 11, 2016). URL: http://www.coindesk.com/blockchain-smarts-contractsreal-world-law/. (дата обращения: 02.03.2025).

[296] Савельев А.И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 46.

[297] Там же. С. 48-53.

позволяет более точно отразить специфику цифровых активов и их значение в современной экономике и праве.

Одной из главных проблем, связанных с информационно-правовым регулированием сделок в цифровой экономике, является обеспечение доверия между участниками сделок, так как в условиях онлайн-торговли и электронных платежей, где отсутствует физическое присутствие сторон, возникают риски мошенничества, несанкционированного доступа к конфиденциальным данным и других противоправных действий[298]. Правовое регулирование должно обеспечивать защиту интересов участников сделок и предотвращать возможные нарушения.

Обсуждая методы правового регулирования в пространстве цифровых технологий, стоит взглянуть на Концепцию комплексного регулирования отношений в сфере цифровой экономики, разработанную с участием некоммерческой организации «Фонда развития центра разработки и коммерциализации новых технологий» на основании данных, полученных от ФГНУ «Институт законодательства и сравнительного правоведения при Правительстве РФ»[299].

Из документа выявляются основные направления для укрепления правового поля цифровой экономики:

— формализация закона;

— определение ключевых принципов цифровой экономики на уровне законодательства. Это может включать важные положения об обработке и защите данных, о правах электронной сделки и другие сферы, которые нуждаются в законодательном урегулировании.

— стратегический национальный контроль;

---

[298] Данное положение подтверждается обширной судебной практикой, в частности постановлением Арбитражного суда Поволжского округа от 18.05.2023 № Ф06-3649/2023 по делу № А55-7445/2022 // СПС «КонсультантПлюс».

[299] Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. М.: Фонд развития центра разработки и коммерциализации новых технологий, 2020. 32 с.

— организация и координация усилий на уровне страны для поддержки цифровой инновации и интеграции, управление национальными проектами и инициативами в области цифровой экономики;

— регулятивное воздействие на уровне подзаконных актов;

— установление руководящих принципов и правил на уровне, который не достигает формализации закона, но является важным для упорядочения отношений и процессов в цифровой экономике;

— стратегическая региональная политика;

— формирование и реализация политик на местном уровне, которые ориентированы на учет специфики регионов и обеспечение роста цифровой экономики с учетом региональных потребностей и ресурсов.

Разработка законодательной базы, нацеленной на цифровую экономику, предполагает создание специфических нормативных документов. Эти документы играют роль фундамента для цифровой экономики и подобны нормативной базе.

В России в настоящее время формируется новая правовая политика, направленная на развитие основных институциональных форм сопровождения экономических отношений в цифровой форме, при этом особое внимание уделяется реализации концепции сервисного государства и цифрового государственного контроля. Такие изменения предполагают создание цифровых форм взаимодействия между властью и бизнесом с помощью государственных и муниципальных услуг, а также институтов фискального цифрового контроля[300].

С точки зрения проблем применения существующих норм права к сделкам, совершаемым в информационной среде, можно рассмотреть понятие токена в контексте российской правовой доктрины ценных бумаг и цифровой экономики. В настоящий момент существуют различные точки зрения и определения токена как ценной бумаги, некоторые авторы (например, Л.А. Новоселова[301]) рассматривают токены как бездокументарные ценные бумаги или цифровые обозначения права на

[300] Овчинников А.И., Фатхи В.И. Цифровые права как объекты гражданских прав // Философия права. 2019. № 3 (90). С. 104-112.

[301] Новоселова Л.А. Токенизация объектов гражданского права // Хозяйство и право. 2017. № 12 (491). С. 29-44.

объект права, что означает, что токены, подобно ценным бумагам, удостоверяют имущественные права, но не требуют физического наличия документа. Вместо этого права на токены записываются и хранятся в цифровой форме, используя технологию блокчейн или другие аналогичные технологии. Это определение позволяет воспринимать токены как электронные эквиваленты прав собственности, передаваемые, обмениваемые или функционирующие в рамках цифровой реальности. А.И. Савельев характеризует токены как «цифровые обозначения права на объект права», которые он также называет «цифровыми ценными бумагами»[302]. В соответствии с его интерпретацией, токены являются электронными версиями прав собственности, которые могут быть переданы или обменяны в электронной среде. Такое определение подчеркивает, что токены представляют собой электронные записи, хранящие информацию о правах и обязанностях их владельцев, могут быть использованы для представления различных видов имущественных прав, таких как право собственности, право на получение дивидендов или право на участие в голосовании. Определение А.И. Савельева отражает сущность токенов в контексте цифровой экономики и рассматривает их как инструменты, позволяющие осуществлять цифровые транзакции и управлять имущественными правами в цифровой среде.

Одними из наиболее актуальных проблем правоотношений в сфере регулирования осуществления сделок в цифровой экономике являются проблемы идентификации сторон при осуществлении сделок в цифровой экономике и обеспечения сделочной безопасности. В связи с этим возникают проблемы, связанные с определением того, как деятельность транснационального бизнеса соотносится с национальным законодательством, поскольку деятельность транснациональных компаний может оказывать влияние на работу национальных законов.

17 мая 2018 года в рамках Петербургского международного юридического форума был проведен круглый стол на тему «Идентификация участников

[302] Савельев А.И. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений // Закон. 2018. № 2. С. 36-51.

правоотношений в цифровой среде и новые цифровые сервисы: тренд на цифровую экономику». В ходе работы форума сопредседатель центра исследований в области защиты неприкосновенности частной жизни при Брюссельском свободном университете К. Кунер, отметил, что законы отстают от технологий, и наличие протекционизма в некоторых странах свидетельствует о боязни государства потерять контроль. С другой стороны, заместитель директора Департамента финансовых технологий Банка России И. Зимин, утверждает, что технологии и закон должны развиваться параллельно, чтобы обеспечить безопасную среду и дальнейшее развитие экономики, приводит пример Закона № 482-ФЗ, который предоставляет возможность удаленной идентификации и разработан не только для финансовых организаций. Вице-президент, начальник департамента АО «Газпромбанк» Т. Кузьмина, отмечает, что удаленная идентификация имеет свои преимущества, такие как сокращение расходов банков и использование электронной подписи, но также указывает на ограниченный круг операций, которые сегодня разрешены законодательством, и отсутствие надежной защиты данных в случае их компрометации. Таким образом, можно сделать вывод, что существует разделение мнений относительно взаимодействия технологий и законодательства в цифровой экономике. Некоторые эксперты считают, что законы должны адаптироваться к технологическим изменениям, чтобы обеспечить развитие и безопасность, в то время как другие полагают, что протекционизм и отставание законодательства свидетельствуют о боязни потери контроля со стороны государства[303].

О.А. Пучков отмечает, что как для физических лиц, так и для юридических лиц, цифровая идентификация становится все более важной, особенно в контексте участия в социальных, экономических и юридических процессах. По мнению О.А. Пучкова, первой проблемой является то, что существующая концепция удостоверения личности в цифровом мире является сложной и многоступенчатой.

[303] На ПМЮФ обсудили идентификацию в цифровой среде. URL: https://www.advgazeta.ru/novosti/na-pmyuf-obsudili-identifikatsiyu-v-tsifrovoy-srede/ (дата обращения: 02.03.2025).

Этот процесс требует множества этапов проверки и аутентификации данных, что может быть неудобным и времязатратным для пользователей.

Следующая проблема заключается в том, что многие люди испытывают стресс, связанный с необходимостью генерировать, запоминать и воспроизводить имена пользователей, пароли и ответы на системные вопросы. Дополнительно, предоставляя свои данные, пользователи теряют контроль над ними, не зная, как долго они будут доступны в цифровом пространстве и могут ли эти данные быть использованы в коммерческих целях. Кроме того, важной проблемой является отсутствие доверия между режимами идентификации и системами запроса на идентичность, что проявляется особенно остро при осуществлении сделок в цифровой экономике. Различные системы, такие как государственные услуги, торговля и финансы, требуют множества как цифровых, так и физических данных для каждой услуги, что создает дополнительные неудобства для пользователей. Это порождает сложность в их взаимодействии с различными цифровыми платформами, требующими различных форм идентификации для каждой конкретной услуги[304]. Можно сделать вывод, что хотя цифровое представление личности является необходимым и важным, существуют проблемы, связанные с его реализацией и необходимо разработать более удобные и безопасные методы цифровой идентификации, чтобы обеспечить удобство и защиту данных пользователей в цифровом пространстве.

Можно обратиться к специальному регулированию отношений, связанных с идентификацией лиц. Например, «Положение об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» является нормативным документом, регулирующим процесс идентификации лиц при совершении сделок. Согласно этому документу, банковские учреждения несут обязательство проводить процедуру идентификации своих клиентов, включая их

[304] Пучков О.А. Идентификация субъектов в цифровом пространстве: несколько правовых проблем // Правопорядок: история, теория, практика. 2019. №1 (20). С. 6-9.

делегатов, лиц, получающих выгоду от сделок, а также конечных владельцев. Это означает необходимость верификации личности данных индивидов путем сбора достоверных сведений о них, это может включать данные паспорта, информацию о месте проживания и другие факты, критически важные для подтверждения личности. Основная задача данной идентификации заключается в предотвращении отмывания преступных доходов и препятствия финансированию террористической деятельности. Идентификация позволяет кредитным организациям проверить, не связаны ли клиенты с преступными деятельностями или террористическими организациями, и предотвратить возможное финансирование таких деятельностей. Положение устанавливает требования к процедуре идентификации, включая сроки проведения идентификационных мероприятий, порядок хранения полученных данных, а также обязанности кредитных организаций по обновлению информации о клиентах[305].

В целом, существующий правовой режим идентификации лица при совершении сделок в цифровой экономике в России имеет некоторые недостатки. Так, физические лица не имеют возможности выбирать данные, которые они хотели бы передать контрагенту. Кроме того, технические процессы аутентификации, такие как в банковской и коммунальной сферах, неудобны для пользователей и часто повторяются. Существующий режим идентификации не гарантирует 100 % надежности и эффективности процесса идентификации. Возможным решением может стать цифровая аутентификация, которая предлагает лучшую структуру данных для идентичности, но это требует изменения традиционных средств данных о личности и расширения возможностей цифровой идентификации с использованием биометрических данных сторон и их представителей по выработанному стандарту, таких как распознавание лиц, радужной оболочки глаза и так далее, а также содержать условие отступления от запрограммированного алгоритма исполнения при наступлении обстоятельств,

[305] Положение об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма / утв. Банком России 15.10.2015 № 499-П. (ред. от 20.07.2016). URL: https://sudact.ru/law/polozhenie-ob-identifikatsii-kreditnymi-organizatsiiami-klientov-predstavitelei/.

независящих от сторон. Будущее идентификации лежит в цифровой аутентификации с использованием биометрических данных, и важно, чтобы российское законодательство своевременно урегулировало этот процесс, например, выработало единый стандарт.

Важным вопросом информационно-правового регулирования отношений по осуществлению сделок в цифровой экономике является проблема правовой защиты участников сделок.

В феврале 2022 года Правительство РФ, при участии в обсуждении регулирования криптовалютного рынка Минфина России, Банка России, Росфинмониторинга России, ФСБ России, МВД России, ФНС России, Минэкономразвития России, Генеральной прокуратуры РФ, утвердило Концепцию законодательного регламентирования механизмов организации оборота цифровых валют[306]. Концепция предлагает несколько мер для защиты прав и интересов инвесторов в области криптовалют:

– разделить инвесторов на квалифицированных и неквалифицированных, что позволит предоставить различные условия для каждой группы;

– внедрить систему лицензирования для криптовалютных площадок, которые обязаны будут обеспечить финансовые гарантии безопасности и достаточности капитала. Такие меры будут способствовать защите интересов граждан.

Реализация данных положений Концепции предположительно позволит создать необходимую нормативную правовую базу, которая выведет индустрию криптовалют из тени и создаст возможности для легальной предпринимательской деятельности. Формирование легального рынка также обеспечит защиту прав физических и юридических лиц, контроль операций с соблюдением требований ПОД/ФТ и способствует привлечению новых участников экономической деятельности, которые будут уплачивать налоги и страховые взносы, что в результате приведет к увеличению доходов бюджета.

---

[306] Концепция законодательного регламентирования механизмов организации оборота цифровых валют // Российская газета. URL: https://rg.ru/2022/02/08/pravitelstvo-utverdilo-koncepciiu-oborota-kriptovaliut-v-rossii.html (дата обращения: 02.03.2025).

Смарт-контракт — это набор программных механизмов, реализованных в виде кода, который выполняется в рамках информационной системы. Основной задачей смарт-контракта является формализация и автоматизация исполнения договоренностей между сторонами, устраняя потребность в посредниках и ускоряя весь процесс заключения и выполнения обязательств.

Американский специалист в сфере информационной безопасности и криптографии, Н. Сабо, является одним из пионеров этой концепции. Его вклад в развитие теории смарт-контрактов положил начало их практическому применению и дальнейшему развитию в рамках криптографических и блокчейн-технологий.

В 1994 году данный термин был введен им для обозначения смарт-контракта как электронной версии договорных отношений между участниками, обладающей встроенной функцией исполнения установленных условий[307]. Смарт-контракт можно рассматривать как самостоятельный контракт, условия которого фиксируются, реализуются и контролируются при помощи компьютерного кода в рамках специализированной программной инфраструктуры.

Смарт-контракты вносят инновации в процесс заключения и выполнения договорных обязательств с помощью блокчейн-технологий. Они позволяют участникам сделки определять условия, которые затем исполняются автоматически, исключая необходимость привлечения посредников или использования централизованных систем управления[308].

Смарт-контракты выделяются высокой степенью открытости и устойчивости к вмешательствам, поскольку их условия фиксируются непосредственно в блокчейн-сети. Данные условия становятся видимыми для всех пользователей, вовлеченных в систему, и не поддаются одностороннему изменению — любые корректировки возможны лишь при общем согласии всех сторон, что существенно повышает уровень доверия и снижает риск несанкционированных изменений.

---

[307] Сабо Н. Смарт-контракты. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (дата обращения: 02.03.2025).

[308] Березина Е.А. Использование смарт-контракта как правовая технология: отечественная и зарубежная законодательная практика // Правовое государство: теория и практика. 2021. № 1 (63). С.97-118.

Также стоит отметить, что смарт-контракты могут быть использованы в различных областях, включая финансовый сектор, недвижимость, логистику и даже государственные услуги, предлагают новые возможности для автоматизации и оптимизации процессов, снижения затрат и повышения эффективности.

В зарубежных исследованиях, посвященных смарт-контрактам, преобладает мнение о том, что они тесно связаны с технологией блокчейна, но дискуссия не касается сущностных аспектов, а сконцентрирована на проблематике использования смарт-контрактов в различных сферах человеческой деятельности. Например, Ким Чан Хи считает, что автоматическое принудительное исполнение смарт-контрактов ассоциируется с самопринуждением и возникает вопрос о правовом обосновании отсутствия возможности восстановления исходного состояния, даже при наличии судебного решения[309].

В Германии на данный момент отсутствует законодательная база, регулирующая смарт-контракты. Несмотря на все их потенциальные преимущества и возможности, существуют серьезные проблемы, которые могут возникнуть в случае, когда самоисполняемость смарт-контракта противоречит действующему законодательству. Применение технологии блокчейн в форме смарт-контрактов для целей аренды недвижимости может вступить в конфликт с нормами Германского гражданского кодекса. Согласно статье 543 Кодекса, договор аренды может быть расторгнут без уведомления, при задолженности за два арендных периода. Таким образом, использование смарт-контракта для автоматической блокировки доступа к арендуемому жилью будет незаконным, с точки зрения немецкого законодательства. Кроме того, такая автоматическая блокировка может создать бытовые проблемы, когда арендатор не сможет получить доступ к своим вещам в квартире или не сможет заботиться о своих близких или животных, которые могут находиться внутри.

В США правовая практика, касающаяся использования смарт-контрактов, только начинает развиваться. Из-за особенностей правовой системы США, каждый

---

[309] Changhee K. Legal Studies of Private Enforcement Accompanied by Smart Contracts. The Institute of Legal Studies Inha University, Inha Law review, 2019, vol. 22, no. 1, pp. 465–494. Available at: http://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE07995518#none.

штат разрабатывает и принимает законы в этой области самостоятельно. В 2017 году штат Аризона стал первым штатом, который принял закон, разрешающий использование смарт-контрактов в торговле и исключающий возможность оспаривания юридической силы договора только на основании того, что в нем используются условия смарт-контракта. Этот закон также приравнял подписи, созданные с помощью блокчейн-технологии, к электронным подписям, которые широко применяются в электронном документообороте[310].

В отличие от ряда стран, которые пока не внедрили законодательные изменения, направленные на признание смарт-контрактов юридически значимыми, в Нидерландах сложилась иная практика. По голландскому гражданскому праву заключение сделки не регламентируется особыми формами—контракт допускается оформлять любым способом, в том числе через программный код в среде блокчейн[311].

Правовая система Нидерландов, таким образом, рассматривает смарт-контракты как полноценные гражданско-правовые соглашения. Для признания их действительными не требуется введения специальных процедур или нормативных предписаний, что облегчает их использование в правовом обороте.

Впервые понятие «смарт-контракт» получило закрепление в законодательстве Республики Беларуси в 2017 году с целью создания благоприятной правовой среды для использования и развития новых технологий, включая блокчейн и смарт-контракты[312]. Смарт-контракты обладают законной силой и признаны юридически действительными наравне с традиционными контрактами, позволяя сторонам вступать в обязательства и выполнять их через данные автоматизированные соглашения. Дополнительно, законодательство

---

[310] Закон Штата Аризона № 2417 от 29.03.2017. URL: https://legiscan.com/AZ/text/HB2417/id/1588180 (дата обращения: 07.07.2025).

[311] Schemkes F. et al. Blockchain en het recht: Een verkenning van de reguleringsbehoefte. Tilburg, 2019.

[312] Приложение 1 к Декрету Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» в п. 9 перечня используемых терминов и их определений содержит следующую дефиницию смарт-контракта: «программный код, предназначенный для функционирования в реестре блоков транзакций (блокчейне), иной распределенной информационной системе в целях автоматизированного совершения и (или) исполнения сделок либо совершения иных юридически значимых действий». [Электронный ресурс] // Национальный интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0 (дата обращения: 07.07.2025).

регламентирует нормы, которые признают электронную подпись, сгенерированную посредством смарт-контракта, за юридически значимую и имеющую обязывающую силу. Это означает, что электронные подписи, оформленные через использование смарт-контрактов, могут применяться в правовых документациях и коммерческих операциях. Закон также предусматривает некоторые требования к проведению и использованию смарт-контрактов, включая обязательное размещение контрактов в блокчейне и обеспечение доступа к информации для всех участников сделки.

Технология блокчейн, на которой основаны смарт-контракты, обеспечивает прозрачность, безопасность и автономность сделок. Основными преимуществами смарт-контрактов являются их юридическая чистота, скорость исполнения, постоянный контроль и сокращение затрат на посреднические услуги. Однако смарт-контракты имеют и некоторые недостатки. Например, невозможность внесения изменений в содержание контракта, неопределенная связь между сторонами контракта и материальными активами на основе существующих платформ.

Одной из главных проблем, которая возникает, является контроль за этими сетями и технологиями. Участники предпринимательской деятельности не удовлетворены текущими методами контроля, но государство имеет большой интерес в этом вопросе, в связи с чем необходимо найти компромиссное решение, которое будет оптимальным с правовой точки зрения и удовлетворит все стороны. Кроме того, платформа блокчейн имеет разнообразные функциональные возможности, и поэтому нет одного юридически выверенного определения, которое бы полностью отражало правовую практику. Однако важно, чтобы любая технология блокчейн определяла порядок хранения данных и обеспечивала доверие участников в их подлинности. В целом правовые возможности всегда сопровождаются рисками и коллизиями в различных областях и необходимо разработать оптимальные правовые конструкции и формы регулирования, чтобы

найти компромисс между интересами участников предпринимательской деятельности и государства[313].

Смарт-контракт, в юридическом аспекте, представляет собой договор между участниками, который зафиксирован в виде компьютерного кода и работает на базе технологии блокчейн, что гарантирует автоматическое выполнение условий контракта при возникновении условий, оговоренных заранее[314]. Такое определение делает невозможным приравнивание смарт-контрактов к классическим договорам. Важно отметить, что не каждый смарт-контракт может быть квалифицирован как соглашение, а то, что воспринимается в контексте программирования, не всегда будет восприниматься как юридическое соглашение сторон. Следовательно, мы можем говорить о двойственности правового режима смарт-контракта, объединяющего в себе характеристики правового документа и технологической разработки.

Отличия условий смарт-контракта от условий классического договора имеют важное значение при изучении его природы. Договор необходим для защиты интересов сторон, и его содержание всегда зависит от согласования позиций этих сторон. Поэтому невозможно оформить договор без предварительных согласований, которые делают ясными все юридически значимые моменты. Только после того, как все условия будут согласованы, можно переходить к их кодированию, что в свою очередь поддерживает модель смарт-контракта, применимую к аналогичным договорам с похожими условиями.

Если допустить возможность указания логических отступлений от исходного договора в смарт-контракте, стоит отметить, что создание договора, который предусматривал бы существенные изменения обстоятельств, ограничено самой природой смарт-контракта. Смарт-контракт не способен учитывать такие оценочные категории, как «добросовестность», «значимость» или «существенность», которые часто являются важными при интерпретации и

---

[313] Левчук С.В. Актуальные проблемы использования смарт-контрактов в предпринимательской деятельности // Экономика. Право. Общество. 2022. Т. 7. № 1 (29). С.16-22.

[314] Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94-117.

применении классических договорных соглашений. Эти категории требуют гибкости и субъективной оценки, что противоречит природе смарт-контрактов, которые ориентированы на четкие, заранее запрограммированные условия и автоматическое исполнение.

В контексте структурирования условий обычного литерального соглашения стоит рассмотреть возможность их интеграции в структуру смарт-контракта через процесс текстовой формализации.

Условия заключенного договора могут быть систематизированы в две основные категории: первая – программируемые элементы, которые поддаются выражению через логические операции в коде, такие как конструкции if/then, позволяют четко кодифицировать и автоматизировать выполнение в рамках смарт-контракта. Вторая категория – не поддающиеся программированию условия, их нельзя адекватно отобразить средствами программирования. К этой категории относятся, например, положения о взаимной ответственности участников соглашения, критерии, базирующиеся на субъективном суждении, а также условия, затрагивающие добросовестность или важность определенных действий.

Важно понимать, что хотя первая категория прекрасно адаптируется к рамкам цифровых контрактов за счет своей анонимности, вторая ставит перед разработчиками задачу размышления о необходимости и способах интеграции юридически значимых, но неформализуемых, пунктов в рамках технологии блокчейн. Этот вопрос является краеугольным в совмещении классического договорного права с инновационными цифровыми механизмами, и его решение требует не только технических, но и правовых инноваций, включая возможное дополнение и развитие законодательной базы[315].

Учитывая уникальные характеристики работы смарт-контрактов, необходимо принимать адаптивную позицию при урегулировании споров,

[315] Clack, Christopher D., Bakshi, Vikram A., Braine, Lee. Smart Contract Templates: Foundations, Design Landscape and Research Directions. URL: https://www.researchgate.net/publication/305779577_Smart_Contract_Templates_foundations_design_landscape_and_research_directions_CDClack_VABakshi_and_LBraine_arxiv160800771_2016 (дата обращения: 02.03.2025).

согласно действующему законодательству и прецедентам в этой сфере. Важно различать два основных типа условий для смарт-контрактов:

– условия, исходящие непосредственно из блокчейна (где действия и выполнение контракта происходят в автономной децентрализованной системе);

– условия, получаемые из внешнего мира, которые реализуются через использование оракулов – сервисов, предоставляющих информацию для исполнения смарт-контракта извне.

Необходимо акцентировать внимание на разнообразии смарт-контрактов с учетом источника данных, влияющих на их выполнение. Они делятся на внутренние, зависящие исключительно от действий, предпринимаемых в контексте самого блокчейна, и внешние, чье исполнение обусловлено факторами за пределами его структуры.

К примеру, в первой категории находятся смарт-контракты, контролирующие доступ к программному продукту. Здесь исключительно внутренние взаимодействия участников в блокчейне определяют исполнение контракта — внешние условия не оказывают на него влияния. Операции активации или блокирования доступа являются наиболее распространенными сценариями применения такого типа смарт-контрактов.

Вторая категория охватывает ситуации, в которых реализация смарт-контракта основывается на информации из внешнего мира. Как пример — контракты, управляющие логистическими процессами, где факты о состоянии груза, сроках и условиях его доставки необходимы для автоматического исполнения данных договоренностей. В этих случаях работа контракта связана с внешними сенсорами или системами отслеживания, что добавляет слой сложности и требует точного соответствия реалий физического мира цифровым показателям в блокчейне.

Такие договоренности несут в себе определенные риски из-за того, что их выполнение не гарантируется согласием участников в блокчейн протоколе и подвержено факторам вне контроля заинтересованных сторон.

Таким образом, смарт-контракты, зависящие от внешних факторов, не могут быть полностью децентрализованными, так как их исполнение выходит за рамки возможностей протокола, что влечет за собой определенные риски и не гарантирует автоматического выполнения всех обязательств.

В мире цифровых технологий смарт-контракты можно систематизировать, разделив на две главные группы. Первая включает в себя те смарт-контракты, которые действуют в рамках уже установленных и оформленных традиционных договорных отношений. Здесь код функционирует как инструмент реализации договора, ускоряя и упрощая выполняемые процессы, но сам по себе не имеет юридической силы. В данной ситуации смарт-контракт представляет собой программу, интегрированную в блокчейн, которая автоматизирует выполнение сторонами своих обязательств. Однако правовая значимость такого соглашения все равно остается за официально оформленным документом, а код смарт-контракта не несет в себе правовых последствий[316].

Вторая группа включает смарт-контракты, которые являются не только техническим инструментом, но и составной частью договора или представляют собой его форму. В этом случае условия, которые могут быть автоматизированы, записываются в виде кода, и смарт-контракт рассматривается как полноценная форма договора. Такой контракт может быть самодостаточным и его исполнение зависит от заранее определенных алгоритмов, встроенных в код.

Чтобы гарантировать юридическую защиту для всех сторон, в случае конфликтов или непредвиденных обстоятельств, крайне важно, чтобы письменный документ договора интегрировал в себя все аспекты и стимуляции, заложенные в структуре соответствующего смарт-контракта, а также полностью соответствовал текущим юридическим нормам. В ситуациях, когда дело доходит до судебного разбирательства, акцент делается на традиционном, письменном договоре. Это объясняется тем, что судебные инстанции склонны опираться на традиционные юридические документы, а не на программный код, который требует

[316] Тюльканов А. Смарт-контракты – договоры или технологические средства? URL: https://zakon.ru/blog/2017/04/07/smart-kontrakty__dogovory_ili_tehnicheskie_sredstva (дата обращения: 02.03.2025).

специфических знаний для интерпретации и, может быть, не полностью понятен в рамках судопроизводства без обращения к квалифицированным экспертам.

Смарт-контракт вполне может быть рассмотрен в качестве технического механизма, гарантирующего выполнение обязательств. Согласно п. 1 ст. 329 Гражданского кодекса Российской Федерации, для обеспечения исполнения договорных обязательств возможно использование не только законом предусмотренных способов, но и таких, которые определены в самом договоре. Таким образом, если стороны договора заблаговременно определили смарт-контракт как способ обеспечения выполнения их соглашения, то это придает ему юридическую значимость как одному из методов исполнения обязательств.

Признание смарт-контрактов как законных и юридически допустимых обеспечений обязательств остается предметом дискуссий среди профессионалов. Основным условием для законности такого рода электронных соглашений является способность точно определить и описать объект обязательств в соответствии с юридическими основаниями. Кроме того, требуется обеспечить, чтобы смарт-контракт удовлетворял всем применимым требованиям законодательства. С учетом того, что основания для возникновения обязательств могут проистекать как из положений Гражданского кодекса Российской Федерации, так и из иных правовых актов, перечень условий, при которых может возникнуть обязательство, не может считаться исчерпанным.

Чтобы смарт-контракт был признан как форма обеспечения обязательства, например, залоговое, необходимо, чтобы его код включал и безоговорочно соответствовал положениям, обозначенным в действующем законодательстве. Это требует от разработчиков таких контрактов не просто технической грамотности, но и глубокого понимания юридических аспектов обязательств, что обеспечивает правовую четкость и защиту сторон в цифровом пространстве[317].

Не менее важно, чтобы намерения участников сделки были ясно зафиксированы при формировании смарт-контракта, который обязан отображать

[317] Карапетов А.Г. Договорное и обязательственное право (общая часть): постатейный комментарий к ст. 307-453 ГК РФ / А.Г. Карапетов [и др.]. М.: Статут, 2017. С. 34.

все ключевые аспекты договоренности и гарантировать юридическую защиту для всех сторон.

Смарт-контракт может функционировать как подтверждение замыслов участников соглашения, не зафиксированных непосредственно в тексте основного контракта, особенно когда он оформлен в стандартной письменной манере, согласно положениям второго пункта 431 статьи Гражданского кодекса РФ. В данных обстоятельствах смарт-контракт может выступать в качестве дополнительного инструмента, способствующего выявлению реальных намерений участников в случаях неоднозначности или отсутствия явных формулировок таких намерений в тексте основного документ.

В ситуации, когда контракт предусматривает переход актива посредством смарт-контракта, данное действие может быть истолковано как принятие предложения через конклюдентные действия (в соответствии с пунктом 3 статьи 438 Гражданского кодекса Российской Федерации). Следовательно, выполнение условий контракта посредством использования смарт-контракта будет рассмотрено как взаимное согласие участников на условия договора в форме, которая исключает необходимость в их подтверждении через обычную письменную формализацию.

В контексте правового аспекта смарт-контракты можно воспринимать не просто как набор программных алгоритмов, но как полноценные электронные договоры со всеми вытекающими правовыми обязанностями и последствиями. Это предполагает, что программный код смарт-контракта обладает достаточной юридической силой, чтобы действовать как самостоятельная форма договорного соглашения, аналогичная традиционным бумажным документам. Следовательно, при наличии соответствующих условий и соблюдении юридических процедур, смарт-контракты обретают режим договоров, способные инициировать юридически значимые действия и инкрустировать принципы расчетов и обязательств в свой код.

Однако весьма вероятно, что соглашение может быть оформлено в цифровом виде через механизм смарт-контракта, и это будет отвечать требованиям

законодательно установленной формы для заключения контрактов. В таких обстоятельствах смарт-контракт не просто выполняет функцию обеспечения выполнения условий договора, но и сам приобретает юридическую значимость, при условии, что все критерии для его признания валидным контрактом удовлетворены.

Согласно доктрине гражданского пара под формой сделки понимается способ выражения воли сторон. В силу положения части 1 статьи 434 ГК РФ, договор может быть заключен в любой форме, если законодательством не установлена обязательная форма. Согласно части 2 этой же статьи, договор может быть заключен обменом электронными сообщениями, что означает признание электронного обмена информацией надлежащей формой сделки. Это позволяет использовать электронные средства для заключения соглашений, в том числе через смарт-контракты.

Поскольку смарт-контракты часто заключаются без явного участия сторон в процессе их исполнения, возникает опасение, что такие соглашения могут не полностью отвечать требованиям законодательства, если условия договора не зафиксированы должным образом и не соответствуют традиционным юридическим стандартам.

В связи с этим, законодательство должно учитывать роль информационных технологий в процессах заключения и исполнения сделок.

Остро стоит вопрос применяемого права при рассмотрении споров с иностранным элементом, а также вопрос понуждения к исполнению решения.

Иной проблемой является сложность определения правового режима кода.

Необходимо выработать единые требования и правила к форме электронных документов, с целью автоматизации проверки наполнения смарт-контрактов.

Одной из ключевых составляющих смарт-контрактов является автоматизация исполнения условий договора, что обуславливает необходимость соблюдения определенных требований, установленных законодательством. Автоматизация, с одной стороны, значительно упрощает процесс исполнения обязательств, но с другой – вызывает вопросы о пределах этой автоматизации и ее

соответствии традиционным правовым нормам. Существует сложность в определении взаимоотношений между принципом свободы заключения договоров, гарантированным статьей 421 Гражданского кодекса Российской Федерации, и установленными правилами в законодательстве[318]. Суть проблемы кроется в том, что программный код, лежащий в основе смарт-контрактов, может быть интерпретирован как вид «закона», созданного отдельными индивидуумами или участниками соглашения и не отражающего волю государства. Это порождает дискуссию о том, должен ли цифровой код иметь приоритет над обычными законодательными нормами, которые устанавливают правила поведения сторон.

Вопрос о юридической иерархии между техническими решениями, используемыми в рамках общественных отношений, и нормами права, существующими в реальном мире, был поднят в одном из решений Федерального Верховного суда Германии по делу № XII ZR 89/21[319]. В материалах дела рассматривался случай, когда французский банк использовал блокчейн для оформления соглашения об аренде батарей для электромобилей. В соответствии с положениями договора, банк имел возможность отключения электропитания батареи в случае нарушения условий контракта, что осуществлялось посредством встроенного компьютера авто. Однако суд пришел к решению, что подобная блокировка автоматическим способом аккумулятора противоречит основным нормам гражданского законодательства, защищающим право собственности и связанное с ним право собственника на свободное использование его имущества.

Согласно абзацу 1 статьи 858 Германского Торгового Уложения, никто не может ограничивать право владельца на владение вещью, за исключением случаев, предусмотренных законом[320]. Таким образом, любое вмешательство в право владения вещью без законных оснований рассматривается как нарушение этого положения. В рассматриваемом деле суд пришел к выводу, что автоматическое отключение батареи, предусмотренное договором, является нарушением прав

---

[318] Керимов Д.А. Законодательная деятельность советского государства. М.: Госюриздат, 1995. С. 87.

[319] URL: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/ document.py?Gericht=bgh&Art=en&nr= 131670&pos=0&anz=1 (дата обращения: 02.03.2025 г.).

[320] Торговое уложение Германии. Закон об акционерных обществах. Закон об обществах с ограниченной ответственностью. Закон о производственных и хозяйственных кооперативах. М.: Волтерс Клувер, 2009. 632 с.

владельца, и признал такое положение контракта недействительным. Суд отметил, что не имеет значения, в какой форме осуществляется воспрепятствование праву владения — физической или виртуальной (например, с помощью электронных механизмов), это не меняет сути нарушения.

Одна из проблем, связанных с использованием смарт-контрактов, заключается в том, что они формулируются на языке программирования, что может вызвать сложности при проверке их содержания на предмет соответствия законодательным нормам.

Поскольку смарт-контракты часто оперируют сложными алгоритмическими конструкциями и многочисленными условиями, обеспечение их правовой защищенности и юридической надежности сопряжено со значительными трудностями. Одним из путей решения обозначенных вопросов может стать внедрение стандартов для подобных цифровых соглашений. Процесс стандартизации предполагает формирование унифицированных положений для различных типов договоров, а также установление норм их практического применения.

Создание типовых моделей смарт-контрактов, которые обладают возможностью адаптации к конкретным обстоятельствам сделки, позволит участникам рынка гибко реагировать на нештатные ситуации и минимизировать риски, связанные с неопределенностью алгоритмов в неожиданно изменившихся условиях.

Результатом такой работы может стать создание банка верифицированных программных продуктов, которые будут доступны для использования в реальных сделках. В этом случае смарт-контракты будут предварительно проверены и соответствовать юридическим требованиям, что снизит риски юридических споров.

Реализация баз данных специфического типа для смарт-контрактов иногда может внести сложности в процесс их верификации, особенно когда требуется разработка смарт-контрактов, предназначенных для эксклюзивных транзакций. Особенность таких контрактов заключается в их уникальности: даже применяя

стандартные модули, каждый смарт-контракт обретает свой особенный набор свойств. Это, в свою очередь, влияет на процедуру аудита и подтверждения правильности функционирования контракта, делая ее более сложной и затратной по времени за счет необходимости тщательного контроля каждой индивидуальной особенности.

Также при использовании смарт-контрактов предлагается закрепить необходимость обязательного применения механизма цифровой идентификации сторон на основе биометрических данных сторон или их представителей по выработанному стандарту, который предусматривает эвентуальность отступления от запрограммированных условий при наступлении непредвиденных обстоятельств, для разрешения проблемы идентификации при дистанционном взаимодействии.

Скорее всего, для верификации таких соглашений потребуется создание сообществ квалифицированных юристов (по типу саморегулируемых организаций).

§ 3.3. Правовое обеспечение информационных отношений в инвестиционной сфере

Цифровые платформы играют ключевую роль в современной экономике, обеспечивая стандартизацию процессов и взаимодействие между различными агентами, делают экономические процессы более современными, быстрыми и инновационными, упрощают коммуникации и предлагают новые возможности для создания стоимости.

Понятие «платформенное право» возникло как ответ на потребность в правовом регулировании взаимодействия на цифровых платформах. Это новое направление развития права, которое обеспечивает интеграцию инновационных цифровых технологий и искусственного интеллекта. Правовые платформы представляют собой комплекс единых принципов, правил, законов и стандартов, которые обеспечивают взаимодействие участников и юридическое сопровождение

различных видов деятельности, они должны быть способны к саморазвитию и самосовершенствованию.

Платформенное право является обобщающим понятием для регулирования платформ и платформенных решений, оно находится в стадии формирования и представляет собой новый этап в развитии права, который регулирует принципиально новые общественные отношения, возникающие в цифровой экономике[321].

Применение платформенных технологий значительно трансформирует множество сфер, начиная от научного поиска и заканчивая экономическим развитием, особенно в динамических инновационных отраслях. Законодательное регулирование таких систем ставит своей целью упорядочение взаимодействий различных экосистем и объединение прогрессивных информационных технологий, стремясь к балансу между интересами всех участников общественной жизни.

Особый акцент законодательства делается на том, чтобы цифровые платформы функционировали честно и эффективно, что существенно для их законной операционной деятельности. Например, включение краудфандинга облегчает процесс сбора средств, повышая его прозрачность и доступность, в итоге снижая расходы на совершение сделок. Это имеет колоссальное значение для роста малого и среднего бизнеса, стартапов.

Краудфандинговые платформы становятся мощным инструментом для сбора капитала на реализацию разнообразных инициатив, позволяя общественности влиять на развитие тех проектов, которые они находят полезными или привлекательными. К тому же, благодаря этой модели, предприниматели могут измерить общественный интерес к их предложениям, что становится важной составляющей в формировании бизнес-стратегий и принятии руководящих решений.

Краудфандинг не только позволяет собирать денежные средства, но и предоставляет информацию о предпочтениях и ожиданиях потребителей,

---

[321] Кашкин С.Ю., Алтухов А.В., Пожилова Н.А. Платформенное право как инструмент инновационных инвестиционных платформ (краудфандинг) // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 1. С. 157-166.

обратную связь, которая является бесценной для любого проекта. При этом система вознаграждений за участие может варьироваться от материальной выгоды (например, продукты или услуги) до морального удовлетворения или признания, что стимулирует активное участие и усиливает вовлеченность в процесс.

Таким образом, краудфандинг обретает статус одного из ключевых компонентов цифровой экономики, оказывая значительное воздействие на инновационные начинания, бизнес-практики и социальные проекты. Платформы служат инструментом демократизации финансирования, способствуют эффективности коммерческой деятельности и раскрывают новые горизонты для проектов, которые иногда невозможно было бы финансировать традиционными способами.

Развитие краудфандинга как альтернативного источника финансирования в России и в мире важно для стимулирования предпринимательской активности, особенно в условиях сложной макроэкономической ситуации, что актуально для малого и среднего бизнеса, которые могут испытывать трудности с получением традиционного банковского или государственного финансирования.

Тем не менее, хотя краудфандинг предоставляет определенные выгоды, он также несет в себе опасности. К ним относятся возможность выбора недостоверного ресурса для размещения проекта, угроза ухудшения деловой репутации организатора при нарушении обязательств перед спонсорами и вероятность присвоения собранных денег самим инициатором. Вдобавок следует подчеркнуть подверженность краудфандинговых платформ киберугрозам, таким как взломы, что выделяет потребность в строгом контроле данной сферы для обеспечения защиты прав всех участников[322].

В связи с вышеуказанными рисками, крайне важным является создание современного и адаптивного законодательства для управления краудфандингом. Это способствует снижению негативных последствий возможных неудач и способствует поддержанию стабильности и динамичного прогресса в сфере таких инвестиций. В целом краудфандинг является важным инструментом в современной

[322] Там же.

экономике, который требует соответствующего правового регулирования для обеспечения его эффективного и безопасного использования.

Центральный банк Российской Федерации разрабатывает стратегии для облегчения взаимодействия между финансовыми институтами и пользователями их услуг. Ключевой задачей является увеличение доступности электронных и дистанционных способов получения финансовых услуг через внедрение удаленных методов продажи данных услуг и продуктов, опирающихся на прогрессивные информационные технологии. В числе предполагаемых к введению мер находится создание системы регистрации, которая обеспечит более простую процедуру верификации личности клиентов при использовании разнообразных финансовых продуктов и сервисов. В результате, клиентам больше не придется проходить дополнительную идентификацию при взаимодействии с новыми продавцами финансовых услуг. Целью этих мер является облегчение доступа к финансовым услугам и продуктам, а также повышение удобства и безопасности для клиентов. Упрощение процесса взаимодействия с финансовыми организациями и использование современных технологий помогут сделать финансовые услуги более доступными и эффективными для всех участников рынка.

В 2016 году совместно Служба по защите прав потребителей финансовых услуг Банк России признала необходимость разработки нормативного регулирования краудфандинговых платформ в России. Для этого было предложено внедрить комплекс мер, охватывающий следующие ключевые аспекты: установление регламентов для деятельности самих краудфандинговых платформ, включая четкие требования к их владельцам и управляющему персоналу; формулирование условий, которые должны выполнять эмитенты ценных бумаг и заемщики, работающие через такие платформы; разработка требований к кредиторам и инвесторам, использующим краудфандинговые платформы для финансирования проектов.

С 2015 года Банк России проводил добровольное анкетирование краудфандинговых платформ, что позволило определить ключевые факторы, способствующие росту рынка краудфандинга, а также выявить основные риски,

связанные с его функционированием. На основе полученных данных была разработана стратегическая дорожная карта по переходу к регулированию краудфандингового сектора. Данный план регулирования был согласован с положениями «Основных направлений развития финансового рынка Российской Федерации на период 2016–2018 годов»[323].

В январе 2018 года Центральный банк Российской Федерации и Минэкономразвития РФ представили проекты закона о краудфандинге, предлагая комплексный подход к регулированию этой сферы. Законопроекты охватывали аспекты, связанные с инвестиционным краудфандингом, включая выпуск токенов в рамках первичного предложения (ICO). Однако краудфандинговые модели, основанные на пожертвованиях и не предполагающие инвестиционного характера, не вошли в сферу регулирования данных документов[324].

В предложенных законопроектах нет специфических упоминаний технологии блокчейн, что отражает стремление разработчиков поддерживать технологически независимый подход. Ключевая идея заключалась в формировании законодательства, способствующего свободному технологическому прогрессу и инновациям. В рамках этого законодательство должно быть спроектировано так, чтобы оно не ограничивалось на конкретных технических решениях, а вместо этого обеспечивало широту выбора и возможность применения самых современных и эффективных технологий для достижения поставленных целей.

Принцип технологической нейтральности находит свое отражение во многих юридических актах Российской Федерации, особенно в отношении информационных технологий и процессов электронного обмена документами. Законы, такие как Федеральный закон «Об электронной подписи»[325] и Федеральный закон «Об информации, информационных технологиях и о защите

---

[323] Разработана концепция регулирования краудфандинга в России. URL: https://www.cbr.ru/press/event/?id=712. (дата обращения 03.08.2023).

[324] ЦБ и Минэкономразвития собрались по-разному регулировать краудфандинг. URL: https://lenta.ru/news/2018/01/29/crowdfunding/ (дата обращения: 08.07.2025 г.).

[325] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Российская газета. 08.04.2011. № 75.

информации»[326], подчеркивают, что законодательство не должно создавать преград для использования определенных технологий и должно способствовать свободе выбора оптимальных технологических решений.

Тем не менее, на пути практического воплощения данного принципа могут возникать сложности. Это может создавать барьеры для внедрения инноваций, так как новые технологические решения вынуждены соответствовать критериям, которые уже не отражают современные реалии. В результате, законодательство, формально провозглашающее технологическую нейтральность, на деле может препятствовать эффективной адаптации к быстро меняющимся техническим и рыночным условиям.

Относительно понятия смарт-контракта, законопроект ЦБ РФ сослался на предыдущий законопроект «О цифровых финансовых активах», где смарт-контракт определяется как договор[327]. Однако в данном законопроекте ЦБ РФ смарт-контракт рассматривается в контексте обязанности раскрытия его исходного кода, то есть как программу для ЭВМ.

Операторы инвестплатформ, подпадающие под действие Закона, должны соответствовать ряду требований, таких как: быть инкорпорированными в России, иметь уставный капитал от 5 млн. рублей, утвердить внутренний документ по управлению конфликтами интересов, обеспечить невозможность внесений изменений инвестором в инвестиционную платформу информации о переходе, возникновении и прекращении утилитарного цифрового права и другие.

Большинство из этих требований можно считать разумными и понятными. Однако, размер ограничения инвестиций в размере 50 тыс. рублей на один проект требует обоснования и обсуждения.

Таким образом, законопроекты о краудфандинге представляли собой системный подход к регулированию краудфандинга. Однако некоторые аспекты,

---

[326] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Российская газета. 29.07.2006. № 165.

[327] Проект Федерального закона № 419059-7 «О цифровых финансовых активах» (ред., внесенная в ГД ФС РФ, текст по состоянию на 20 марта 2018). URL: http://sozd.parliament.gov.ru/bill/419059-7 (дата обращения: 07.12.2024).

такие как неинвестиционный краудфандинг и размер ограничения инвестиций, требуют дальнейшего обсуждения и уточнения.

Также неквалифицированный инвестор может поучаствовать за год лишь в 10 таких проектах или вложить не более 500 тыс. руб. Сумма сборов для проекта также ограничена. Одна платформа, в случае принятия закона, не сможет собирать более 200 млн рублей. Закон «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации»[328] установил ограничение для неквалифицированных инвесторов в сумме до 600 тыс. руб. в год. Данное ограничение, помимо квалифицированных инвесторов, не касается также граждан, зарегистрированных как ИП, и граждан, которые покупают утилитарные цифровые права (далее - УЦП) по договорам инвестирования, заключенным с публичным акционерным обществом. В законодательстве предусмотрено, что одно юридическое лицо в течение года может привлекать инвестиции через инвестиционные платформы на сумму, не превышающую 1 миллиард рублей. Однако это ограничение не затрагивает публичные акционерные общества, использующие для привлечения средств выпуск цифровых финансовых активов и утилитарных цифровых прав. Данные категории эмитентов исключены из общего ограничения, что предоставляет им более широкие возможности для работы с инвестициями в цифровом пространстве.

Закон № 259-ФЗ, принятый 2 августа 2019 года, является ключевым документом для законодательного регулирования краудфандинга в Российской Федерации[329]. Он вносит существенный вклад в формирование правового поля для сферы привлечения инвестиций через инвестиционные платформы, обеспечивая разработку универсальных оснований для их функционирования. Применительно

---

[328] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

[329] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

к операторам таких платформ, документом определяются ключевые требования к профессиональной деятельности, налагаются обязательства об информационной прозрачности перед инвесторами, а также устанавливается ответственность за несоблюдение установленных норм и правил.

С другой стороны, несмотря на значительные усилия по регулированию этой области, закон не покрывает все аспекты краудфандинга. Например, не в полной мере регулируются вопросы, связанные с защитой прав инвесторов, особенно малоопытных и непрофессиональных. Также в законе отсутствуют четкие регулятивные рамки для краудфандинг-платформ, работающих с благотворительностью или социальными проектами.

В целом этот закон является важным инструментом в регулировании краудфандинга в России, но его можно считать лишь первым шагом на пути к созданию более полного и детального регулирования этой отрасли. В дальнейшем потребуется проведение дополнительной работы по уточнению и дополнению нормативной базы в этой области.

ЦБ РФ в своем обзоре 2022 года указал на то, что рынок краудфандинга в России демонстрирует высокие темпы роста. Так, объем привлеченных средств через краудфандинговые платформы значительно увеличился с 7 млрд рублей в 2020 году до 13,8 млрд рублей в 2021 году и только за первый квартал 2022 года было инвестировано свыше 3 млрд рублей. При этом количество компаний, получивших право заниматься краудфандингом, также активно растет: на момент публикации обзора на рынке действовал уже 61 оператор инвестиционных платформ. Также в 2021 году был отмечен рост по объему сделок и охвату клиентской базы.

Краудлендинг, предоставление коллективных займов под финансирование проектов, является наиболее распространенным видом краудфандинга, особенно привлекателен для субъектов малого и среднего бизнеса, которым требуется быстрое и кратковременное пополнение оборотных средств. В 2021 году на долю этого сегмента пришлось 64% привлеченных средств, а в первом квартале 2022 года было заимствовано 2,29 млрд рублей.

Вторым по распространенности видом краудфандинга является краудинвестинг, коллективное инвестирование в компании через покупку их ценных бумаг. В 2021 году эмитенты смогли привлечь 4,74 млрд рублей, а за первый квартал 2022 года - 1,06 млрд рублей[330].

Объем рынка краудфандинга в 2022 году вырос на 1,5 раза и достиг отметки в 20,4 млрд рублей. К началу 2023 года в реестр операторов инвестиционных платформ были включены 64 организации, а количество зарегистрированных инвесторов на этих платформах составило 54,6 тыс. Более 90% из них являются неквалифицированными инвесторами.

Относительно рынка цифровых прав, можно отметить, что он только начинает свое развитие. Так, к началу 2023 года в реестр операторов информационных систем, выпускающих ЦФА (цифровые финансовые активы), включены сведения о трех организациях. Каждый из этих операторов разместил на своей платформе не менее четырех выпусков ЦФА, а в качестве эмитентов выступили 11 компаний из различных сфер деятельности.

Банк России продолжает активно работать над совершенствованием регулирования рынка платформенных сервисов. Он призывает к установлению прозрачных правил и обязательному соблюдению операторами требований по безопасности и надежности предоставляемых сервисов[331].

Сокращение традиционных источников финансирования и снижение доступности инвестиционного капитала способствуют распространению краудфандинга как инновационного инструмента привлечения средств. Усиление конкурентной борьбы между провайдерами инвестиционных платформ мотивирует их совершенствовать предлагаемые сервисы. Благодаря этим факторам, российский рынок краудфандинга демонстрирует динамику роста и становится все более привлекательным для малых и средних предприятий, а также

---

[330] Обзор рынка краудфандинга в России. URL: http://www.cbr.ru/collection/collection/file/42097/crowdfunding_market_01_2022.pdf (дата обращения 03.08.2023).

[331] Маркетплейсы, краудфандинг и ЦФА: итоги развития платформенных сервисов. URL: https://www.cbr.ru/press/event/?id=14760 (дата обращения 03.08.2023).

для частных инвесторов, расширяя спектр возможностей для каждого из участников.

Согласно действующему законодательству о привлечении инвестиций, лица, причастные к террористическим или экстремистским действиям, а также те, кто не соответствует внутренним правилам краудплатформы, не имеют права получать финансирование. Также запрещено привлечение участников юридических лиц и индивидуальных предпринимателей, имеющих неснятую судимость за экономические преступления и против власти. Другим критерием отказа является дисквалификация руководителя юридического лица или запрет на деятельность для индивидуального предпринимателя после банкротства.

Кроме того, для доступа к площадке потенциальных фаундеров часто проводится скоринг - анализ различных показателей, связанных с их деятельностью. Например, анализируется финансовое состояние, кредитная история и срок деятельности. В связи с этим Банк России рекомендует краудплощадкам разработать регламент проведения такой оценки и рассмотреть возможность привлечения третьих лиц для ее проведения.

Краудплатформы, которые присваивают рейтинги своим проектам, должны разработать внутренний документ с методологией присвоения рейтингов, их сроками и периодичностью, перечнем оцениваемых показателей, основаниями и порядком пересмотра рейтинга, а также возможностью привлечения третьих лиц при необходимости. При формировании шкалы рейтингов Центральный банк не рекомендует использовать обозначения, схожие с теми, которые присваивают международные и национальные рейтинговые агентства, чтобы не запутать потенциальных инвесторов.

Банк России рекомендует публиковать всю указанную информацию бесплатно на главной странице сайта краудплатформы или обеспечить быстрый доступ к ней в хронологическом порядке с указанием даты ее раскрытия и периода актуальности.

Согласно установленному сроку, рекомендации Банка России должны быть выполнены до 31 марта 2023 года. Несмотря на их необязательность,

предполагается, что все лицензированные компании будут использовать эти рекомендации в своей работе[332].

Согласно данным, крупнейшими мировыми рынками краудфандинга в настоящее время выступают Соединенные Штаты Америки, Китай и Великобритания. В США p2p-кредитование занимает доминирующее положение, составляя 94% совокупного объема краудфандингового рынка. Остальная доля приходится на краудинвестинг (2%) и краудфандинг, основанный на вознаграждениях (2%).

При подготовке российского Закона о привлечении инвестиций был проведен анализ международной практики, особенно в тех юрисдикциях, где краудфандинговые механизмы развиваются наиболее стремительно, таких как Англия, США и Китай. Использование опыта этих стран позволило учесть проверенные подходы к регулированию рынка и адаптировать их к российским реалиям.

Среди региональных лидеров рынка альтернативного финансирования выделяются Китай в Азиатско-Тихоокеанском регионе, Соединенные Штаты Америки на американском континенте и Великобритания в Европе. На данных рынках наблюдается устойчивое доминирование p2p-кредитования, которое на потребительские цели по-прежнему является крупнейшим сегментом альтернативного финансирования[333].

Ст. 2 Федерального закона от 2 августа 2019 года № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» под краудфандингом понимается как деятельность по привлечению инвестиций путем размещения на

---

[332] ЦБ решил усилить контроль за краудфандингом. URL: https://www.vedomosti.ru/finance/articles/2022/11/22/951451-tsb-reshil-usilit-kontrol-za-kraudfandingom (дата обращения 03.08.2023).

[333] Уварова А.В. Правовое регулирование сделок взаимного кредитования в Российской Федерации и зарубежных странах: дисс. … канд. юрид. наук. М., 2021. С. 8.

сайте инвестиционной платформы предложений о вступлении в гражданско-правовые отношения, направленные на финансирование проектов или компаний[334].

В Соединенных Штатах Америки «Закон о запуске наших бизнес-стартапов» (The Jumpstart Our Business Startups Act or JOBS Act) 2012 года ввел правовую рамку для краудфандинга, позволяя компаниям собирать средства от неквалифицированных инвесторов через интернет-платформы[335]. Однако сам термин «краудфандинг» не определен в тексте закона. В Великобритании Финансовый регуляторный орган (FCA) осуществляет регулирования данной сферы в соответствии с Законом о финансовых услугах и рынках[336].

В целом, и в зарубежной, и в российской практике подчеркивается важность использования Интернета и современных технологий в краудфандинге, но зарубежная практика также акцентируют внимание на использовании открытых исходных кодов и социальных медиа. Оба подхода схожи в том, что краудфандинг направлен на привлечение средств для реализации конкретных проектов или идей, но за рубежом также подчеркивается аспект объединения индивидуумов для достижения общей цели.

В рамках усилий по структурированию и уточнению сферы краудфандинга Международная организация комиссий по ценным бумагам (IOSCO) внесла значимый вклад, выпустив в 2014 году фундаментальный доклад. В этом документе IOSCO предоставила детальную классификацию краудфандинга, выделив его на четыре основных направления: пиринговый (основанный на пожертвованиях), с вознаграждением, краудлендинг (одноранговое кредитование) и акционерный краудфандинг. Такое разграничение предоставляет более ясное представление об отличительных чертах каждого из подходов и их внутренних процессах, что

---

[334] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

[335] Jumpstart our business startups act (2012) P.L. 112-106- APR. 5, 2012. URL: https://www.govinfo.gov/content/pkg/PLAW-112publ106/pdf/PLAW-112publ106.pdf (дата обращения: 08.07.2025).

[336] Financial Services and Markets Act 2000. URL:https://www.legislation.gov.uk/ukpga/2000/8/contents (дата обращения: 08.07.2025).

способствует более глубокому пониманию механизмов работы всей индустрии краудфандинга.

Краудфандинг пожертвований – это форма краудфандинга, где люди добровольно передают деньги или ресурсы для поддержки проекта или идеи, без ожидания финансового возврата. Краудфандинг вознаграждений – это форма краудфандинга, где люди вкладывают деньги в проект в обмен на некоторую форму вознаграждения, которое обычно связано с проектом. Пиринговое кредитование – это форма краудфандинга, где инвесторы предоставляют займы лицам или организациям через онлайн платформы, которые соединяют заемщиков и кредиторов. Акционерный краудфандинг – это форма краудфандинга, где инвесторы вкладывают деньги в обмен на акции или долю в компании. Такое разделение подчеркивает разнообразие моделей и подходов в сфере краудфандинга, каждая из которых имеет свои особенности и требует своего подхода в части регулирования и управления.

Рынок альтернативного финансирования, основанный на технологии краудфандинга, развивается стремительно и находит массовое применение по всему миру, что в свою очередь приводит к трансформации модельных типов краудфандинга, что, вероятно, связано с изменением потребностей и предпочтений участников рынка, а также с развитием технологий.

Кембриджский центр альтернативных финансов играет важную роль в исследовании и мониторинге этого рынка, регулярно публикуя отчеты о состоянии индустрии альтернативных финансов. В 2020 году этот центр впервые опубликовал глобальный отчет, что подчеркивает все большую глобализацию этого сектора. Подход, разработанный в Кембридже для категоризации различных форм краудфандинга, был модифицирован М.В. Чудиновским и Ю.В. Куваевой с учетом специфики России (таблица 3)[337]. Необходимость такой адаптации возникла из-за отсутствия устоявшихся научных терминологий в русском языке для многих английских понятий.

[337] Куваева Ю.В., Чудиновских М.В. Мировая практика трансформации подходов к регулированию краудфандингов // Вестник НГУЭУ. 2020. № 3. С. 114-128.

Центральный банк РФ реализует собственный подход к классификации краудфандинга и рассматривает в своих обзорах такие его сегменты как:

– p2p кредитование инвестор и заемщик – физические лица;

– p2b кредитование: инвестор – физическое лицо, заемщик – юридическое лицо;

– b2b кредитование: инвестор и заемщик – юридические лица;

– «rewards»-краудфандинг: средства привлекаются на цели или проекты за нефинансовое вознаграждение.

Таблица 3 – Кембриджский подход к классификации модельных типов краудфандинга[338]

Модельный тип краудфандинга	Предлагаемая русскоязычная терминология
Долговой краудфандинг	
P2P Consumer Lending	Потребительское пиринговое кредитование
P2P Business Lending	Пиринговое кредитование бизнеса
Invoice Trading	Пиринговое кредитование под залог счетов
P2 P Property Lending	Пиринговое кредитование под залог недвижимости
Real Estate Crowdfunding	Краудфандинг недвижимости
Balance Sheet Business Lending	Балансовое бизнес-кредитование
Balance Sheet Consumer Lending	Балансовое потребительское кредитование
Balance Sheet Property Lending	Балансовое имущественное кредитование
Debt based Securities	Краудфандинговое финансирование через долговые ценные бумаги
Mini Bonds	Краудфандинг на основе миниоблигаций
Долевой краудфандинг	
Revenue Sharing	Краудфандинг на основе распределения прибыли
Equity based Crowdfunding	Акционерный краудфандинг
Community Shares	Долевое финансирование сообществ
Reward based Crowdfunding	Краудфандинг вознаграждений нефинансовых
Donation based Crowdfunding	Основанный на краудфандинг пожертвовании

В современной российской финансовой практике понятие краудфандинга было расширено в соответствии с определением, представленным Центральным

[338] Там же.

Банком РФ в документе «Обзор платформенных сервисов в России»[339]. В этом обзоре, который касается деятельности операторов инвестиционных платформ, информационных систем и операторов финансовых платформ, краудфандинг также охватывает процесс приобретения утилитарных цифровых прав (УЦП) и цифровых финансовых активов. Эти расширения в определении краудфандинга позволяют углублять и совершенствовать существующие механизмы привлечения финансирования и инвестиций в цифровую экономику России.

Подход Банка России к классификации сегментов краудфандинга не основан на едином классификационном признаке и вместо этого использует различные критерии для разных сегментов, включая статус инвестора (физическое или юридическое лицо) и сущность экономических отношений. В контрасте с подходом Банка России, международный подход к классификации типов краудфандинга основан на едином классификационном признаке, а именно на сущности экономических отношений. Разница в подходах к классификации может отражать различия в правовых и экономических системах, а также в особенностях рынка краудфандинга в России и в мире.

Федеральный закон «О привлечении инвестиций с использованием инвестиционных платформ»[340] раскрывает перечень форм краудфандинга, которые рассматриваются как подходящие для использования в рамках российской экономики. Среди них находятся предоставление займов, что соотнесено с понятием peer-to-peer кредитования, и два вида инвестиционных механизмов: вложения в эмиссионные ценные бумаги, напоминающие акционерный финансовый вклад, и инвестиции в неэмиссионные ценные бумаги, которыми являются утилитарные цифровые права, схожие с краудфандинговым получением вознаграждений.

---

[339] Обзор платформенных сервисов в России. Операторы инвестиционных платформ, операторы информационных систем и операторы финансовых платформ. Информационно-аналитический материал. М., 2024. URL: https://www.cbr.ru/Collection/Collection/File/49243/platform_services_2024-1.pdf (дата обращения: 02.03.2025).

[340] Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2019. № 31. Ст. 4418.

Однако наблюдается определенное расхождение между концепцией краудфандинга, описанной Центральным Банком России, и основными формами, которые были закреплены законодателем. Ожидается, что с течением времени и развитием самого сектора краудфандинга, законодательство будет дополнено новыми моделями краудфандинга. Это подтверждает готовность краудфандинговой практики развиваться и адаптироваться к меняющимся условиям рынка, а также необходимость актуализации законодательства для отражения этой гибкости и разнообразия подходов к привлечению инвестиций.

Операторы инвестиционных платформ работают на растущем рынке краудфандинга, который начался с народного финансирования проектов и сейчас предоставляет возможность привлечения средств в долг или капитал от множества инвесторов. Деятельность этих платформ регулируется законом «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации»[341] с 2020 года.

Инвесторами на инвестиционных платформах могут быть как физические, так и юридические лица, но только юридические лица и индивидуальные предприниматели могут привлекать инвестиции через такие платформы. В течение года через инвестиционную платформу можно привлечь не более 1 млрд рублей.

Законодательство устанавливает перечень возможностей для инвестирования через инвестиционные платформы, охватывающий широкий спектр инструментов. Это включает в себя краудлендинг, то есть предоставление займов через платформы, инвестирование в различные типы эмиссионных ценных бумаг, за исключением определенных категорий, приобретение таких инструментов, как утилитарные цифровые права, а также вложения в цифровые финансовые активы. Эти механизмы предоставляют инвесторам гибкость и разнообразие вариантов для участия в финансировании проектов и предприятий через современные цифровые каналы.

---

[341] Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2019. № 31. Ст. 4418.

Оператором инвестиционной платформы может быть только организация, внесенная в реестр Банком России. Основные требования к операторам включают наличие российского юридического лица, размер собственных средств не менее 5 млн рублей и соблюдение требований к правилам инвестиционных платформ.

Условия взаимодействия между операторами инвестиционных платформ и их клиентами регулируются правилами инвестиционных платформ, которые определяют порядок работы, способы инвестирования, права и обязанности сторон, размер вознаграждения оператора и другие аспекты. Правила инвестиционной платформы должны быть согласованы с Банком России[342].

Однако возможности для инвестирования через цифровые платформы могут быть ограничены, могут существовать определенные проблемы при попытке расширить эти возможности.

При реализации данного закона могут возникнуть несколько значительных трудностей. Одной из ключевых проблем является отсутствие прямой ответственности операторов инвестиционных платформ за выполнение обязательств, которые принимают на себя привлекающие инвестиции стороны. Это, в свою очередь, может привести к снижению уровня доверия со стороны инвесторов. Также возникает ряд вопросов, связанных с нормативным регулированием взаимоотношений между инициаторами проектов и инвесторами.

Относительная «либеральность» подхода к правовому регулированию краудфандинга может быть обусловлена стремлением создать благоприятные условия для инвестиционных платформ, что позволит им эффективно привлекать коллективное финансирование в перспективные проекты. В данном контексте минимизация государственного контроля над этими процессами рассматривается как способ стимулирования развития новых финансовых инструментов, которые могли бы составить альтернативу традиционному банковскому кредитованию и способствовать их популяризации[343].

---

[342] Операторы инвестиционных платформ. URL: https://www.cbr.ru/finm_infrastructure/oper/ (дата обращения 03.08.2023).

[343] Кашкин С.Ю., Алтухов А.В., Пожилова Н.А. Платформенное право как инструмент инновационных инвестиционных платформ (краудфандинг) // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. №1. С.157-166.

Предусмотренные требования к раскрытию информации операторами инвестиционных платформ направлены на повышение прозрачности всех этапов инвестиционного процесса. В частности, они включают обязательное предоставление сведений об операторе и его деятельности, правила работы площадки, информацию о субъектах, привлекающих инвестиции, а также об условиях заключения договоров и инвестирования. Кроме того, операторы обязаны раскрывать полную информацию об инвестиционных предложениях, что позволяет инвесторам оценивать риски и принимать более взвешенные решения. Таким образом, эти меры способствуют не только обеспечению прозрачности, но и повышению уровня финансовой грамотности частных инвесторов.

Особенности правового регулирования в РФ включают возложение ответственности в краудфандинговых проектах на инициаторов и площадки. Ст. 12 Федерального закона от 02.08.2019 № 259-ФЗ устанавливает, что оператор инвестиционной платформы несет ответственность за убытки, причиненные вследствие закрытого перечня нарушений и тому подобное[344]. Данная статья закона определяет ответственность оператора инвестиционной платформы в контексте краудфандинга:

1. Оператор инвестиционной платформы несет ответственность за убытки, которые могут быть причинены в результате предоставления недостоверной, неполной или вводящей в заблуждение информации об инвестиционной платформе и самом операторе, что подчеркивает важность прозрачности и честности в деятельности оператора платформы.

2. Оператор также несет ответственность за убытки, вызванные нарушением им правил инвестиционной платформы, подчеркивает важность соблюдения установленных правил и процедур.

[344] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

3. Оператор несет ответственность, если инвестиционная платформа не соответствует требованиям статьи 11 Федерального закона, чем подчеркивает необходимость соблюдения законодательства в деятельности платформы.

В то же самое время, данная статья также уточняет, что оператор инвестиционной платформы не несет ответственности за обязательства лиц, привлекающих инвестиции, то есть оператор не несет финансовой ответственности за инвестиционные риски, которые принимают на себя инвесторы.

Таким образом, данная правовая норма определяет границы ответственности оператора инвестиционной платформы, с одной стороны подчеркивая его ответственность за предоставление достоверной информации и соблюдение правил, а с другой – освобождая от ответственности за риски, связанные с инвестициями.

В свою очередь ст. 9 Федерального закона от 31.07.2020 № 259-ФЗ определяет ответственность оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов следующим образом[345]:

– операторы информационных систем несут ответственность перед пользователями за возмещение убытков, спровоцированных разнообразными обстоятельствами. Среди них — потеря информации, касающейся цифровых финансовых активов и данных их владельцев, неполадки в функционировании IT-технологий и оборудования, предоставление информации, которая является некорректной, неполной или вводит в заблуждение. Также обязанности оператора включают обеспечение соблюдения установленных процедур функционирования информационной системы и ее соответствие нормам, предусмотренным федеральным законодательством;

– в случае сбоя в работе информационных технологий и технических средств, оператор обязан совершить действия, которые были предприняты пользователем и были прерваны из-за этого сбоя.

---

[345] Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

Таким образом, статья устанавливает строгую ответственность оператора за надежное и бесперебойное функционирование информационной системы, защиту данных пользователей и соблюдение законодательства, а также обязывает оператора компенсировать любые убытки, возникшие у пользователей из-за недостатков или сбоев в работе системы.

Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации»[346] включает ряд положений, направленных на защиту прав инвесторов.

1. Обязательства оператора. Закон устанавливает ряд обязательств для оператора инвестиционной платформы, включая обязанность предоставлять достоверную информацию об инвестиционной платформе, своей деятельности и проектах, доступных для инвестирования.

2. Ответственность оператора. Оператор инвестиционной платформы может быть привлечен к ответственности за убытки, возникшие в результате предоставления недостоверных, неполных либо вводящих в заблуждение данных. Кроме того, оператор несет ответственность в случаях нарушения внутренних правил платформы или несоответствия ее работы установленным законом требованиям.

3. Ограничения для инвесторов. Закон также устанавливает ограничения на сумму инвестиций для неквалифицированных инвесторов с целью защиты их от чрезмерных рисков.

4. Регуляторный контроль. Деятельность операторов инвестиционных платформ подлежит контролю со стороны регулятора (в данном случае, Банка России), что также способствует защите прав инвесторов.

Таким образом, закон включает ряд мер, направленных на обеспечение защиты прав инвесторов при привлечении инвестиций с использованием

[346] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

инвестиционных платформ, но, как и любое законодательство, он не может полностью исключить все риски, связанные с инвестиционной деятельностью.

В отношении регулирования защиты прав инвесторов Федеральным законом от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации»[347] можно выделить следующие основные недостатки:

1. Недостаточная защита неквалифицированных инвесторов. Хотя закон устанавливает ограничения на сумму инвестиций для неквалифицированных инвесторов, эти меры могут быть недостаточными для защиты этих инвесторов от чрезмерных рисков.

2. Ответственность операторов. Вопрос об ответственности операторов инвестиционных платформ за убытки инвесторов не полностью разрешен, что может создать проблемы при попытках инвесторов взыскать свои потери.

3. Недостаточный контроль за деятельностью операторов. Несмотря на то, что деятельность операторов подлежит контролю со стороны регулятора, в законе не уточняются конкретные механизмы такого контроля.

4. Риски, связанные с недостатками в области информационной безопасности, прежде всего, связаны с защитой персональных данных.

В России защита персональных данных регулируется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»[348], который применяется и к операторам платформ краудфандинга. В соответствии с положениями закона, операторы обязаны информировать субъектов персональных данных о целях, способах и принципах обработки персональных данных, а также о любых рисках, связанных с передачей данных.

---

[347] Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

[348] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006 г. № 165.

Операторы краудфандинговых платформ несут ответственность за строгое соблюдение принципов и норм в области обработки персональных данных:

1. Осуществление сбора персональных данных может проводиться исключительно после получения явного разрешения от лиц, данные которых предполагается обработать, за исключением случаев, прямо предусмотренных.

2. Защита собранных персональных данных должна осуществляться путем их надежного хранения, предотвращения любых форм несанкционированного вмешательства, включая неправомерный доступ или распространение.

3. Строгое сохранение конфиденциальности персональных данных является обязательным, как и реализация эффективных мер защиты этих данных в процессе их обработки.

4. Предусмотрен свободный доступ для владельцев персональных данных к своей информации, с возможностью вносить изменения или осуществлять удаление своих данных по запросу.

Обязательное исполнение этих требований обеспечивает правовую защищенность участников платформ и вносит доверие в процесс краудфандинга.

Вместе с тем применение этих норм к практике краудфандинга может вызывать сложности из-за особенностей данной сферы, в том числе международного характера многих платформ и проектов. Проблемы конфиденциальности и защиты персональных данных в сфере краудфандинга являются важными и актуальными и можно выделить следующие основные их сегменты:

1. Сбор и хранение персональных данных. Платформы краудфандинга собирают большое количество персональных данных от пользователей, включая имена, адреса, информацию о банковских счетах и другую конфиденциальную информацию, что создает риск утечки данных и злоупотребления информацией.

2. Недостаточная информация о политике конфиденциальности. Платформы краудфандинга могут не предоставлять пользователям достаточно информации о том, как они собирают, хранят и используют персональные данные, что может

привести к нарушению прав пользователей на информационную прозрачность и контроль над своими данными.

3. Отсутствие адекватных мер безопасности. Платформы краудфандинга могут не обеспечивать должного уровня защиты персональных данных от несанкционированного доступа, утечек или взлома, так как законодательно механизм такой защиты в РФ не урегулирован.

4. Несоответствие международным стандартам. Политики и практики в области конфиденциальности и защиты персональных данных на платформах краудфандинга могут не соответствовать международным стандартам, таким как, например, Общий регламент по защите данных (GDPR).

Предлагается дополнить Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации»[349] следующими положениями:

– дополнить главу 2 Федерального закона статьей 11.1 с описанием требований к обеспечению информационной безопасности на инвестиционных платформах;

– установить требование к операторам по проверке достоверности информации, предоставляемой лицом, привлекающим инвестиции;

– дополнить закон требованиями к положению о преодолении потенциальных конфликтов интересов, которые могут возникнуть в деятельности оператора инвестиционной платформы;

– учитывая специфику отношений, предлагается установить обязанность субъекта, привлекающего финансирование, информировать инвесторов о реалистичных стратегиях вложения средств с предоставлением отчетности на различных этапах реализации проекта, а также обязанности заключения соглашения о неразглашении полученной информации до завершения реализации проекта.

---

[349] Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

– внести изменения в статью 7 Закона, с целью упрощения процедуры идентификации инвестора (физического лица) для целей инвестирования посредством инвестиционной платформы (например, интегрировать функционал портала государственных услуг)[350].

§ 3.4. Правовое регулирование использования информации ограниченного доступа в цифровой экономике

При осуществлении экономической деятельности, включая экономическую деятельность в цифровой форме, главенствующую роль играет реализация инструментария информационной безопасности, которая может формироваться на различных уровнях, в том числе, на корпоративном[351]. Наиболее ярко проявленными в экономической деятельности выступают институты коммерческой, банковской и налоговой тайн. Данный набор тайн был выбран в силу принципа экономической значимости сведений, которые выступают содержанием институтов. Формирование данного принципа позволяет структурировать отношения в изучаемых стратах.

В дополнении к обозначенному принципу можно выделить принцип адекватности, который выступает определяющим в вопросе сущностного наполнения при установлении того или иного института тайн.

Говоря про категорию «тайна», необходимо согласиться с позицией А.А. Фатьянова о комплексности и многоаспектности явления, что порождает разные точки зрения в литературе и законодательстве[352]. И.В. Бондарь подчеркнул важность исходя из целостности информации, составляющей тайну, и норм правового режима, которые ограничивают доступ к этой информации. Он утверждает, что для получения обстоятельного и полного понимания тайны

---

[350] Рустамов П.А. К вопросу о совершенствовании правового регулирования краудфандинга в России // Проблемы экономики и юридической практики. 2023. № 1. С. 106.

[351] Малюк А.А., Морозов А.В. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности // Безопасность информационных технологий. Т. 26. № 4. С. 33.

[352] Фатьянов А.А. Тайна как социальное и правовое явление. Ее виды // Государство и право. 1998. № 6. С. 19-28.

необходимо рассмотреть данное правовое явление через призму его формы и сущности в их взаимодействии[353].

Правовой режим коммерческой тайны

Рассматривая вопрос ограничения доступа как способа защиты информации, следует обратить особое внимание на то, как законодатель регулирует право собственника информации на ее защиту.

В соответствии с российскими правовыми нормами, физические и юридические лица, располагающие сведениями профессионального, делового, коммерческого, производственного, банковского или иного характера, которые были приобретены за их собственные средства либо представляют для них самостоятельный интерес, в случае если не затрагиваются охраняемые законом секреты, имеют право самостоятельно определять порядок доступа к таковой информации. Помимо этого, они наделены полномочием относить эти сведения к разряду конфиденциальных и внедрять необходимые механизмы и методы обеспечения их защиты. То есть, право устанавливать соответствующий режим доступа к информации имеют лица (юридические и физические), которые владеют информацией.

Институт коммерческой тайны является ключевым видом конфиденциальной информации при осуществлении субъектами хозяйствования своей деятельности. Именно от него, во многом, определяется успех деятельности экономического субъекта, он прямо коррелирует с основополагающим фактором ведения экономической деятельности – величина получаемой прибыли.

Правовое регулирование исследуемых отношений имеет крепкие исторические традиции. Дореволюционная система законодательства имела юридические нормы, регулирующие вопросы защиты коммерческой тайны (законодательство о защите «секретов промысла»). Именно в этот промежуток времени стали практиковать ведение торговых книг, которые содержали в себе достоверную информацию о состоянии дел хозяйствующего субъекта.

[353] Бондарь И.В. Тайна по российскому законодательству (проблемы теории и практики). Дисс. … канд. юрид. наук: 12.00.01. Нижний Новгород, 2004. С. 25.

Информация из этих книг могла быть разглашена только в некоторых случаях (при отправлении правосудия, при исчислении налогов, в случаях банкротства субъекта хозяйствования и так далее)[354].

Г.Ф. Шершеневич высказывался следующим образом «российское законодательство стремится охранить тайну купеческих книг, их недосягаемость для постороннего глаза», делая вывод о том, что за исключением указанных в законе случаев (споры по делам товарищества, споры по наследованию, споры по банкротству), никто и ни под каким предлогом не вправе требовать, чтобы открыты были торговые книги, составляющую ненарушимую коммерческую тайну»[355].

Данный институт именовался по-разному: «торговая тайна», «промышленная тайны», «тайна кредитных отношений». В.В. Розенберг предложил именовать изучаемый правовой режим конфиденциальной информации как «промысловая тайна», которая, по его мнению, делилась на два института: тайну технических процессов фабрикаций (тайна процессов производства) и тайну коммерческую (тайну распределения благ), данная классификация была реципирована из германского права, однако, прижилась категория «коммерческая тайна»[356].

Во второй половине 19-го века – начале 20-го века стал появляться понятийно-категориальный аппарат исследуемого института. В немецкой правовой науке, как известно, российское право подвержено влиянию романо-германской школы (преимущественно, французской и германской системам права), стали формироваться определение коммерческой тайне, в частности, германское право определяло коммерческую тайну как тайну технических процессов тайны производства благ и тайну их распределения[357].

Принятие в марте 1903 году Уголовного уложения (части его) повлияло на развитие института в Российской империи. Закон содержал в себе раздел 29, именуемый «Об оглашении тайн», который насчитывал 6 составов

---

[354] Северин В.А. Правовое регулирование коммерчески ценной информации // Законодательство. 2000. № 9.С. 36-40.

[355] Шершеневич Г.Ф. Учебник торгового права. М.: «СПАРК», 1994. С. 85.

[356] Розенберг В.В. Промысловая тайна. СПб.: изд. М-ва фин. 1910. С. 12-13.

[357] Розенберг В.В. Промысловая тайна. СПб.: изд. М-ва фин. 1910. С. 12-13.

преступлений[358]. Документ определял фабричную тайну как «особые, употребляемые на заводе, фабрике или в заведении, или предположенные к употреблению приемы производства»[359], под кредитной тайной понимались «сведения, заведомо составлявшие тайну сих (кредитных) учреждений, неподлежащие огласке»[360].

Переходя к советскому периоду истории российского государства, стоит сказать о том, что институт коммерческой тайны был просто уничтожен на этапе становления советской государственности. Само собой, это обуславливается трансформацией экономических процессов, которые проходили в тот период времени.

До середины 1980-х годов в Советском Союзе экономические отношения полностью контролировались государством, которое являлось единственным субъектом хозяйственной жизни. Это изменилось с созданием правовых основ кооперативной деятельности, что стало началом отхода от централизованной экономической модели.

Важным этапом в этом процессе стало упразднение понятия коммерческой тайны 27 ноября 1917 года. Декрет о рабочем контроле признавал всю информацию открытой для общества, что было частью более широких изменений в экономических принципах того времени[361]. Все предприятия были приведены под управление государства, а режим коммерческой тайны был замещен категориями военной и государственной тайны[362].

Ситуация начала меняться в 1980-х, когда в СССР произошли значительные реформы в экономическом законодательстве. Принятие Закона «О кооперации в СССР»[363] 26.05.1988 года и Закона «О предприятиях в СССР»[364] 04.06.1990 года

---

[358] См.: Россий Российское законодательство X-XX веков. В 9 т. Т. 9. / под общ. ред. чл - кор. АЕН РФ, д.ю.н., проф. О.И. Чистякова. М., 1994. С. 271.

[359] Розенберг В.В. Промысловая тайна. СПб.: изд. М-ва фин. 1910. С. 44-49.

[360] Там же. С. 49.

[361] См.: Декреты Советской власти. Т. 1. – М.: Гос. изд-во полит. литературы, 1957. С. 83-85.

[362] См.: Сборник приказов Военного Совета республики. 1918. № 97. С. 987.

[363] Закон СССР от 26.05.1988 г. № 8998- XI «О кооперации в СССР» // Ведомости Верховного Совета СССР. 1988. № 22. Ст. 355.

[364] Закон СССР от 04.06.1990 г. № 1529- I «О предприятиях в СССР» // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР. 1990. № 25. Ст. 460.

инициировало перемены, которые позволили расширить субъектный состав экономической деятельности.

В новой законодательной рамке, особенно в статье 33 Закона о предприятиях, коммерческая тайна была определена как информация, не относящаяся к государственным секретам и связанная с производственной, управленческой, финансовой и другими сферами деятельности предприятия. При этом разглашение такой информации могло повлечь за собой убытки. Решение о том, какая информация должна оставаться конфиденциальной, оставалось за руководством предприятия. Меры по защите таких данных стали значимой частью корпоративной политики и практики.

Эти изменения подчеркивают эволюцию отношения к роли частного сектора и приватизации в советской экономике, предвещая серьезные трансформации в структуре и регулировании хозяйственной деятельности.

Статья 151 Основ гражданского законодательства Союза ССР и республик от 31 мая 1991 года содержала нормы о том, что обладатель коммерческой информации, которая составляет секрет производства (ноу-хау), имеет право на защиту информации от незаконного использования при выполнении ряда условий:

– информация, обладает коммерческой ценностью в силу неизвестности ее третьим лицам;

– доступ к информации ограничен на законном основании;

– применяются надлежащие методы по защите конфиденциальности информации[365].

С принятием Закона об информации в российское законодательство вводится категория конфиденциальной информации, с формированием критерия конфиденциальности[366]. Коммерческая тайна, а также все иные виды тайн, стали образовывать частные примеры конфиденциальной информации. В юридической доктрине существует неразрешенный спор в отношении того, что как соотносится

[365] Основы гражданского законодательства Союза ССР и республик (утв. ВС СССР 31.05.1991 г № 2211-I) // Ведомости СНД и ВС СССР. 1991. № 26. Ст. 733. С.136.

[366] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Российская газета. 29.07.2006. № 165.

коммерческая тайна с секретами производства (ноу-хау) и объектами интеллектуальной собственности. К примеру, А.П. Сергеев полагает, что коммерческая тайна представляет собой самостоятельный объект интеллектуальной собственности, а у лица, владеющие информацией, присутствует субъективное право по отношению к такой информации[367]. В.Ф. Попондопуло полагает, что нормы коммерческой тайны также относятся к объектам интеллектуальной собственности, так как массив информации характеризуется как результат творческой деятельности[368].

Противоположная точка зрения у О.А. Городова. Он, а также подобную точку зрения разделяет И.А. Зенин, считает, что с точки зрения формально-юридической, коммерческая тайна не относится к перечню объектов интеллектуальной собственности, однако, обладает свойствами, которые могут быть отнесены к результатам интеллектуальной собственности[369].

Для понимания особенностей коммерческой тайны нужно отличать ее от института правовой защиты секретов производства (ноу-хау). До 2014 года в науке присутствовала неопределенность в отношении вопроса разграничения категорий коммерческая тайна и ноу-хау. Закон о коммерческой тайне уравнивал информацию, составляющую коммерческую тайну с секретами производства. Гражданский кодекс предусматривал режим коммерческой тайны как обязательный режим для защиты ноу-хау.

В марте 2014 года российское законодательство обогатилось важными поправками, закрепленными в Федеральном законе № 35-ФЗ[370]. Этот акт внес коррективы в несколько частей Гражданского кодекса РФ и другие законы, серьезно повлияв на правовую охрану коммерческой информации и интеллектуальной собственности.

---

[367] Сергеев А.П. Гражданское право. Учебник / Под ред. А.П. Сергеева, Ю.К. Толстого. М., 1998. Ч. 3. С. 169-174.

[368] Попондопуло В.Ф. Коммерческое (предпринимательское) право. Учебник. М.: Юристъ, 2005. С. 178-180.

[369] Городов О.А. Интеллектуальная собственность: правовые аспекты коммерческого использования. СПб, 1999. С. 136.; Зенин, И. А. Основы гражданского права России (конспект лекций для специалистов по праву интеллектуальной собственности). М., 1993. С. 208-215.

[370] Федеральный закон от 12.03.2014 г. № 35-ФЗ «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета. 14.03.2014. № 59.

Фундаментальное значение в нормах права приобрели положения о защите секретов производства (ноу-хау). Данный термин охватывает сведения различного рода — начиная от производственных и технических знаний, заканчивая экономическими и организационными аспектами деятельности, характеризующимися определенной ценностью на рынке из-за их уникальности и недоступность для широкой публики.

Законодатель уточнил, что ноу-хау стоит рассматривать в контексте интеллектуального творчества в научно-технической сфере, устанавливая требования к владельцам таких сведений: необходимость не только доказать их эксклюзивность и ценность, но и предпринять все возможные меры для сохранения конфиденциальности, включая установление режима коммерческой тайны.

Тем самым закон устанавливает прямую связь между ноу-хау и коммерческой тайной, образуя подкатегорию в более широкой категории охраняемой информации. Такое соотношение показывает желание законодателя классифицировать ноу-хау как объект интеллектуальной собственности, что представляет собой следующий шаг в развитии правовой защиты коммерческих информационных ресурсов.

Можно сделать вывод о том, что обладатель секретов производства имеет право, но не обязанность, использовать режим коммерческой тайны. Коммерческую же тайну можно квалифицировать как самостоятельный институт права (информационного и гражданского)[371].

Однако в складывающемся российском законодательстве термин коммерческая тайна не представлялся чем-то новым. Он встречается во множествах нормативных правовых актах, но мало где раскрывался. Совершенно справедливо утверждение Е.К. Волчинской о том, что говорить о сформированости института коммерческой тайны в начале 2000-х не приходиться[372].

---

[371] Информационное право: учебник для бакалавриата, специалитета и магистратуры // Под ред. М.А. Федотова. М.; Изд-во Юрайт, 2019. 497 с.

[372] Волчинская Е.К. Коммерческая тайна в системе конфиденциальной информации // Информационное право. 2005. № 3. С. 17-21.

Наличие подобного правового пробела аргументировало принятие специального нормативного правового акта[373]. Результатом стал Федеральный закон «О коммерческой тайне», который установил должное правовое регулирование в данной области, включая определение понятийного аппарата[374].

К сведениям, отнесенным к коммерческой тайне, относятся любые данные, включая информацию о результатах научно-технической интеллектуальной деятельности и о методах осуществления профессиональной работы, обладающие реальной или возможной экономической ценностью из-за своей недоступности для третьих лиц. К этим сведениям третьи лица не обладают законным доступом, поскольку их обладатель установил специальный режим охраны конфиденциальности[375].

Коммерческая тайна представляет собой установленный режим конфиденциальности информации, который обеспечивает ее владельцу ряд преимуществ. В частности, режим коммерческой тайны позволяет повысить доходность деятельности, минимизировать издержки, удерживать конкурентные позиции на рынке или получать иные виды выгоды, связанные с сохранением информации в закрытом доступе[376].

О.А. Городов выделяет ряд юридически значимых признаков информации, при присутствии которых можно говорить о режиме коммерческой тайны:

- неизвестность третьим лицам;

- недоступность третьим лицам[377].

Законодательство Российской Федерации определяет и регулирует режим коммерческой тайны, обозначая границы и принципы его применения. Закон «О коммерческой тайне» предписывает открытый перечень информации, которую

---

[373] Кокорин И. С., Игбаев З. Р. Развитие коммерческой тайны в России (историко-правовой аспект) // Ленинградский юридический журнал. 2011. № 1. С 94-99. URL: https://cyberleninka.ru/article/n/razvitie-kommercheskoy-tayny-v-rossii-istoriko-pravovoy-aspekt (дата обращения: 14.02.2021).

[374] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // Собрание законодательства Российской Федерации от 09.08.2004. № 32. Ст. 3283.

[375] Информационное право: учебник для бакалавриата, специалитета и магистратуры // Под ред. М.А. Федотова. М.; Изд-во Юрайт, 2019. 497 с.

[376] Информационное право: учебник для бакалавриата, специалитета и магистратуры // Под ред. М.А. Федотова. М.; Изд-во Юрайт, 2019. 497 с.

[377] Городов О.А. Информационное право: учебник для бакалавров. М.: Проспект, 2015. 304 с.

можно классифицировать как коммерческую тайну, одновременно исключая из этой категории ряд важных сведений:

1. Информацию о состоянии и структуре активов государственных и муниципальных унитарных предприятий, а также о расходовании средств из бюджетов соответствующих уровней власти.
2. Сведения, заложенные в документы лицензионного и разрешительного характера для осуществления бизнес-деятельности.
3. Данные о долгах организаций по зарплате и другим социальным обязательствам.
4. Информацию об условиях проведения торгов по приватизации собственности государственного и муниципального уровня.
5. Прочую информацию, детализировано перечисленную в Законе.

За установление режима коммерческой тайны следует не просто декларация о его наличии, а проведение целого ряда защитных. Мероприятий. В соответствии с ч. 1 ст. 10 упомянутого Закона, к таким мерам относятся:

1. Создание подробного списка информации, которая является коммерческой тайной.
2. Ведение учета лиц, имеющих доступ к этой информации, включая тех, кому она была передана.
3. Установка правил доступа к коммерческой тайнам, а также контроль за их соблюдением.
4. Пометка материальных носителей с такой информацией специальным обозначением «коммерческая тайна» с учетом информации о собственнике.
5. Принятие иных обоснованных мер для обеспечения конфиденциальности данных.

Применение этих мер гарантирует юридически значимое закрепление статуса информации как коммерческой тайны и основывает правовые предпосылки для ее защиты.

Коммерческая тайна представляет собой инструмент, которым предприниматель «скрывает» способы осуществления экономической деятельности, дающие ему преимущества на рынке.

Вопрос охраны программного обеспечения на сегодняшний день становится все более значимым, особенно в свете непрерывно растущей информационной ценности и увеличения числа кибератак. Российское законодательство предоставляет возможность использования механизма коммерческой тайны для защиты программного обеспечения, что может включать в себя исходный код, алгоритмы и другие технические и технологические решения, стоящие за продуктом.

Инструменты коммерческой тайны позволяют регулировать доступ к информации и обязывают сотрудников и третьих сторон соблюдать конфиденциальность в отношении охраняемых сведений. В случае программного обеспечения применения таких мер служит дополнительной защитой, наряду с авторским правом, которое обычно представляет основную форму правовой охраны программ для ЭВМ.

При рассмотрении вопросов защиты информации необходимо разграничивать понятия «коммерческая тайна» и «секрет производства (ноу-хау)». В российской правовой системе под коммерческой тайной подразумевается широкий спектр сведений, признаваемых конфиденциальными на основании решения их обладателя. В то же время ноу-хау охватывает главным образом информацию, связанной с техническими разработками и обладающей рыночной значимостью, которая непосредственно относится к результатам интеллектуального творчества в области техники.

Хотя оба понятия направлены на охрану ценной информации, статус ноу-хау предполагает более высокий уровень инновационности и уникальности информации, часто связан с техническими знаниями и технологическими процессами. Таким образом, в контексте программного обеспечения, важно не только классифицировать его как коммерческую тайну, но и учитывать потенциал

его уникальности в качестве ноу-хау, если это возможно, для обеспечения более полного уровня правовой защиты.

В контексте российского законодательства, владелец ноу-хау, в том числе и исходного кода программного обеспечения, вправе принимать «разумные меры» для обеспечения сохранения конфиденциальности этой информации, даже не объявляя ее формально коммерческой тайной. Это подразумевает, что разработчик или владелец такого рода интеллектуальной собственности должен предпринять действия, рассматриваемые в деловой практике и судебной практике как адекватные для защиты значимых данных.

Однако формальное присвоение режима коммерческой тайны информации вида ноу-хау дает дополнительные преимущества. В частности, это упрощает защиту прав в случае юридических споров, так как законодательно утвержденный режим коммерческой тайны создает четкие рамки для доказательства нарушений и помогает обосновать реализацию мер конфиденциальности.

Внедрение законодательных уточнений дало толчок к улучшению практик защиты конфиденциальной информации, обогащая нормативную базу и предоставляя держателям интеллектуальных прав дополнительные инструменты для обеспечения правовой защиты их ноу-хау. Это, в свою очередь, способствует стабильности и надежности владения интеллектуальной собственностью, а также их использовании в экономической деятельности.

Чтобы понять практическое значение этих изменений, можно рассмотреть процесс регулирования информации производственно-технической сферы, которая становится коммерческой тайной. Если ранее введение режима защиты таких данных могло представлять трудности, то теперь, благодаря возможности использования норм Гражданского кодекса и специального законодательства о коммерческой тайне, процесс этот стал более понятным и доступным. При возникновении международных ситуаций эти же механизмы упрощают доказывание в зарубежных юрисдикциях.

Однако подходы к определению коммерческой тайны отличаются в разных правовых системах. В странах, как Германия и Китай, не существует

стандартизированного взгляда на положение коммерческой тайны в контексте гражданского оборота. Там защита коммерческих тайн осуществляется скорее через законодательство, направленное против конкурентных нарушений, что подразумевает акцент на предотвращение недобросовестных практик в бизнесе.

Таким образом, изменения, внесенные в российское законодательство, нацелены на более эффективное регулирование защиты ноу-хау, делая процесс более удобным для правообладателей и повышая интерес к инновационным разработкам в стране. Это предоставляет российским компаниям и предпринимателям укрепленные позиции на международной арене и способствует активной интеграции в мировую экономику[378].

Можно повторить условия введения режима коммерческой тайны:

– необщедоступность информации, составляющей коммерческую тайну;

– фактическая или потенциальная коммерческая ценность;

– принятие правообладателем разумных мер для соблюдения конфиденциальности такой информации.

Отнесение исходного кода к категории необщедоступной информации связано с тем, что пользователи программного обеспечения при его приобретении или лицензировании получают доступ исключительно к объектному коду. Исходный код остается недоступным без специальных действий, таких как декомпиляция, которая, в свою очередь, законодательно ограничена.

Разрешение на декомпиляцию законодательно ограничено и может быть предоставлено исключительно с целью гарантирования бесперебойного функционирования официально приобретенного программного обеспечения. Это правило усиливает конфиденциальный статус исходного кода программ, делая его недоступным для широкой публики и сурово контролируя любые попытки несанкционированного доступа.

---

[378] Терехова Е.В. Трансграничная передача информации, составляющей коммерческую тайну: проблема правовой квалификации // Актуальные проблемы российского права. 2014. № 3. С. 508.

В силу данных ограничений исходный код вполне может быть предметом режима коммерческой тайны, учитывая его закрытый и сенситивный характер. Чтобы обеспечить соответствие требованиям о «разумных мерах» защиты конфиденциальности, рекомендуется явно указывать условия о неразглашении в лицензионных соглашениях, через которые передается информация об исходном коде.

Такие условия служат двойной цели: с одной стороны, они закрепляют обязательства сторон по поддержанию конфиденциальности кода, а с другой – облегчают процесс правоохранительной деятельности при возможном нарушении данных условий. Это также способствует созданию законной и прозрачной среды для распространения программного обеспечения и его обслуживания.

Кроме того, целесообразно предусмотреть договорный запрет на любые действия, направленные на декомпиляцию или иную попытку обратного анализа исходного кода.

В качестве преимуществ можно выделить:

– отсутствие временных рамок на охрану;

– отсутствие участия государства в данном вопросе;

– эвентуальность распространить режим не только на исходный код, но и на дизайн программы (интерфейс)[379].

Для того, чтобы интегрировать режим коммерческой тайны в процесс распространения программного обеспечения, необходимо принять несколько ключевых мер. Первоначально требуется ограничить доступ к тем фрагментам пользовательского интерфейса программы, которые подлежат защите как коммерческая тайна.

Дополнительно, для укрепления защиты конфиденциальности, рекомендуется составление специальных соглашений о неразглашении с клиентами, которые дополнят основные договоренности, касающиеся передачи прав на использование программного продукта. Альтернативный вариант

[379] См.: Computer Care v. Service Sys. Enters., Inc., 982 F.2d 1063, 1074 (7th Cir. 1992) (full text).

заключается в интегрировании положений о конфиденциальности непосредственно в лицензионные договоры и другие связанные с распределением ПО документы. Это обеспечит юридическую защищенность исходного кода и связанных с ним элементов, предоставляя правообладателю лучшие гарантии соблюдения их исключительных прав[380].

Можно сделать вывод, что сущностные характеристики правового института коммерческой тайны определяются информационным и экономическим потенциалом.

Информационный потенциал раскрывается в следующих признаках

– конфиденциальный характер сведений, отнесенных к коммерческой тайне;

– ограничение возможности доступа к ней;

– осуществление мероприятий по ее сохранности;

Экономический потенциал сведений, отнесенных к коммерческой тайне:

– наличие легальных преференций перед участниками конкурентной деятельности в сфере производства, реализации товаров, выполнении работ, оказании услуг;

– наличии у информации ценностных характеристик для конкретно-определенного субъекта хозяйствования.

Правовой институт коммерческой тайны представляет собой совокупность обособленных правовых норм, регулирующих общественные отношения по поводу формирования, использования и защиты информации, составляющей коммерческую тайну субъекта.

Данный институт характеризуется своей комплексностью, так как тесно взаимосвязан с нормами международного, конституционного, гражданского, информационного, трудового права. Комплексность правового института вытекает из комплексности информационного законодательства, а также дополняется

[380] How Can You Protect Your Software As A Trade Secret? URL: https://www.khlawfirm.com/how-can-you-protect-your-software-as-a-trade-secret/ (дата обращения: 06.10.2024).

комплексностью метода правового регулирования (диспозитивного и императивного).

Стоит упомянуть про субъектов коммерческой тайны. Положения Закона о коммерческой тайне[381] не позволяют удовлетворить потребности коммерческого взаимодействия, так как являются ограниченными и не охватывают все общественные отношения, которые существуют. Соответственно, образуются реперные точки соприкосновения общественных отношений, регулирование которых осложняется.

В качестве основных субъектов можно выделить владельцев тайны (собственники) и конфидентов (лица, которым информация стала известна в силу исполнения обязанностей). Объединяющим элементом для конфидентов выступает то, что информация для них является вторичной (становится известна от владельца), а также то, что они ограничены в правомочиях по использованию этих сведений. Конфидентов можно разделить на группы лиц: 1) работники; 2) контрагенты; 3) представители государственной власти; 4) иные лица (аудиторы, адвокаты и так далее)[382].

Полноценное функционирование правового института, его жизнеспособность, напрямую зависит от инструментария принуждения. Одним из таких инструментариев является ответственность за невыполнение требования закона. Для регулирования вопросов охраны коммерческой тайны УК РФ в статье 183 устанавливает ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. В данном конкретном случае законодатель приравнивает эти три вида тайн, так они наполненными, преимущественно, одними и теми массивами данных. Правовой режим охраны трансформируется в момент поступления информации к определенному субъекту (например, при поступлении информации в налоговый орган, на сведения начинает распространяться режим налоговой тайны). В

[381] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // Собрание законодательства Российской Федерации от 09.08.2004. № 32. Ст. 3283.

[382] Беляев М.В. Объекты и субъекты права на коммерческую тайну : автореф. дис. … канд. юрид. наук: 12.00.14. М., 2005. 10 с.

зависимости от умысла и степени вреда варьируется и степень наказания (назначение штрафа либо (и) лишение свободы).

Гражданско-правовая ответственность в сфере коммерческой тайны возникает за нарушение норм главы 75 части четвертой ГК РФ, Закона о коммерческой тайне и иных правовых актов, регулирующих отношения в данной области. Способы защиты можно разделить на юрисдикционные и неюрисдикционные. К юрисдикционным относятся действия уполномоченных государственных органов по защите нарушенных либо оспариваемых прав, под неюрисдикционными понимаются самостоятельные действия гражданина или организации по защите своих прав.

Стоит отметить, что прекращение отношений с организацией (например, увольнение, сокращение) не влечет за собой прекращение ответственности, за исключением дисциплинарной.

Дисциплинарная ответственность выражается в увольнении работника в соответствии с пп. «в» п. 6 ч. 1 ст. 81 ТК РФ.

Административная ответственность выражается в применении штрафных санкций, предусмотренных ст. 13.14 КоАП РФ.

Рассматривая вопросы ответственности, важно включить анализ положений, которые законодательство устанавливает для регулирования отношений в сфере защиты ноу-хау и механизмов коммерческой тайны. Гражданский кодекс Российской Федерации четко определяет последствия нарушения исключительных прав на секреты производства. Как указывается в статье 1472 ГК РФ, ответственность возлагается не только на тех, кто без права получил доступ к секретной информации и ее использовал или разгласил, но также на тех, кто взял на себя обязательства сохранять такую информацию в секрете, согласно статьям 1468, 1469 или 1470 ГК РФ, и не исполнил эти обязательства. В случае нарушения исключительного права нарушитель обязан возместить причиненные убытки, кроме ситуаций, когда закон или договор не предусматривают другой вид ответственности.

Основной акцент в вопросах нарушения прав на ноу-хау делается на неправомерное действие с информацией, обладающей реальной или потенциальной коммерческой ценностью, что представляет собой две главные формы: незаконное использование и разглашение таких сведений. Под нарушителями понимают лиц, которые получили доступ к ноу-хау недозволенным путем, а также тех, кто по условиям соглашений должен был сохранять данные в тайне, однако не выполнил взятые на себя обязательства. Законодательство четко обозначает рамки нарушений в области ноу-хау, ограничивая их использованием или разглашением защищаемой информации, не относя к нарушениям другие возможные действия.

Поскольку ноу-хау обладает коммерческой ценностью, его применение для целей, не связанных с извлечением прибыли или производственными процессами, представляется маловероятным. По сути любое использование ноу-хау происходит в рамках деловой или производственной деятельности, и именно это делает его объектом правовой охраны.

Программное обеспечение, предназначенное для широкого распространения, может столкнуться с определенными трудностями при попытке классифицирования его как коммерческой тайны, несмотря на формальные основания для такой защиты. Наличие общедоступного пользовательского интерфейса и ограниченный доступ к исходному коду — условия, обычно установленные в рамках авторского права, — создают риски.

В этих условиях предпочтительнее обеспечивать защиту в виде коммерческой тайны для тех программных продуктов, которые применяются исключительно внутри самой компании-разработчика. Примеры такого ПО включают системы, контролирующие промышленные процессы, управляющие специализированным оборудованием или программы, основанные на работе искусственных нейронных сетей. Эти программные продукты зачастую не только содержат деловые секреты компании, но и критически важны для поддержания ее конкурентных преимуществ и инновационной деятельности.

В таких случаях доступ к исходному коду контролируется более жестко, что позволяет лучше обеспечить его конфиденциальность и защиту от декомпиляции. Такой подход снижает риск оспаривания режима коммерческой тайны и увеличивает уровень защиты интеллектуальной собственности[383].

К проблемам данного правового института коммерческой тайны можно отнести отсутствие правового режима электронных документов и невозможность распространения режима коммерческой тайны на конфиденциальную информацию в отношении сотрудника, который был уволен до введения такого режима, а также невозможно обязать подписать соглашение о неразглашении, в соответствии со ст. 1467 ГК РФ[384].

Правовой режим банковской тайны

Институт банковской тайны выступает в качестве гаранта основных прав и свобод человека и гражданина, которые реализуются через конституционную норму о праве каждого на уважение его личной и семейной тайны, неприкосновенности частной жизни. В настоящее время практика не содержит в себе четкого определения банковской тайны. Статьи с соответствующим названием имеются в ГК РФ (ст. 857), а также в специальном законе – Федеральном законе от 02.12.1990 № 395-1 «О банках и банковской деятельности»[385], однако, они определяют банковскую тайну через провозглашение института как такового либо через перечисление обязанностей, а также сопутствующих видов тайн, что, по мнению автора, только усиливает сложности трактования данного института. Кроме того, набор различных описательных элементов не влияет на сущностные характеристики категорий. Можно сделать предположение об идентичности категорий, а также необходимости их проработок к той части, которая раскрывает содержание понятия. На неопределенность содержания института банковской тайны указывает и практика Конституционного Суда РФ, которая подчеркивает

---

[383] Поляков Д.Н. Комбинированные механизмы правовой охраны программного обеспечения в трансграничной предпринимательской деятельности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 3. С. 243-250.

[384] Анцупов Д.В. Актуальные изменения и проблемы коммерческой тайны // Образование и право. 2016. № 1. С. 197-200.

[385] Ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» // Ведомости съезда народных депутатов РСФСР от 06.12.1990 г. № 27. Ст. 357.

обязанность федерального законодателя формировать единую правовую базу РФ, формировать законодательство о банковской тайне в едином русле для недопущения возникновения правовых коллизий, а также затрагивания частных и публичных интересов[386].

Изучение данного правового института следует начать с рассмотрения истории развития банковской тайны в Российском государстве.

Основы института банковской тайны в России уходят корнями во времена до революции. Уже в 1862 году были законодательно закреплены принципы конфиденциального обращения с коммерческой информацией: в «Положении о городских общественных банках» в разделе 1, статье 9, говорилось о том, что с момента назначения на должность руководители и весь персонал банка обязаны были давать письменное обязательство о неразглашении личных коммерческих дел и счетов клиентов[387].

Эволюция данного института нашла свое дальнейшее выражение в Уставе Государственного Банка 1895 года[388]. В статье 22 этого Устава наложение обязанности по сохранению банковской тайны распространялось на всех работников банка, включая членов его совета.

После Октябрьской революции 1917 года произошла смена экономических принципов, что повлекло за собой и преобразования в понимании и регулировании банковской тайны в СССР. Период советской власти ознаменовался активным использованием понятия «тайна вклада», которое охватывало защиту информации о банковских счетах, вкладах и проводимых с ними операциях.

Значимую роль в поддержании конфиденциальности банковской информации играло «Положение о государственных трудовых сберегательных кассах», принятое в 1925 году, которое закрепило за собой уголовную

---

[386] Постановление Конституционного Суда РФ от 14 мая 2003 г. № 8-П «По делу о проверке конституционности пункта 2 статьи 14 Федерального закона «О судебных приставах» в связи с запросом Лангепасского городского суда Ханты-Мансийского автономного округа» // Российская газета. 27.05.2003 г. № 99.

[387] Положение о городских общественных банках (утв. 10.06.1862 г.) // Полное собрание законов Российской империи. Собр. II. Т. XXXVII. № 38362. СПб., 1862. 834 с.

[388] Арефа Н.И. Устав Государственного Банка. СПб., 1895. 306 с.

ответственность за разглашение банковских секретов среди работников финучреждений[389].

В тот же период были определены органы, которым разрешалось доступ к информации о банковских вкладах. Это были следственные и судебные органы, а правомочия выделялись соответствующим законодательством. Дополнительные изменения произошли с принятием в 1927 году Постановления ЦИК и СНК РСФСР «О принципах построении кредитной системы», которое расширило круг лиц, обладающих правом запроса банковской информации. В частности, данное постановление предоставило Госбанку полномочия запрашивать у кредитных организаций сведения о задолженностях лиц и о счетах госорганов, что значительно расширило рамки банковской тайны[390].

Наряду с этим, ЦИК и СНК внес изменения в «Положение о кооперативном кредите» 1927 года, ограничив право судебных и следственных органов получать справки о вкладах только в случае, если органы осуществляют уголовное производство в отношении данных лиц[391]. Можно предположить, что подобные правовые гарантии носили декларативный характер, были нацелены на повышение доверия граждан в финансовой системе, несмотря на общий тоталитарный контроль со стороны государства.

Важно подчеркнуть, что в советской практике конфиденциальность финансовых операций обеспечивалась не только для индивидуальных граждан, но и для компаний и организаций. Именно такие принципы нашли отражение в Положении о государственных трудовых сберегательных кассах СССР, где защита распространялась на различные виды вкладчиков, включая как физических, так и юридических лиц[392]. Этот документ, таким образом, закрепил широкий охват

---

[389] Постановление Президиума Центрального Исполнительного Комитета. Положение о государственных трудовых сберегательных кассах Союза Советских Социалистических Республик. 27 ноября 1925 г. // Распубликовано в № 278 Известий ЦИК Союза ССР и ВЦИК от 5 декабря 1925 г.

[390] Постановление Центрального Исполнительного Комитета и Совета Народных Комиссаров СССР. О принципах построения кредитной системы. СЗ СССР. 1927. № 35. Ст. 364.

[391] Постановление ЦИК и СНК. Положение о кооперативном кредите. 18.01.1927 г. // Распубликовано в № 20 Известий ЦИК Союза ССР и ВЦИК от 26.01.1927 г.

[392] Постановление Президиума Центрального Исполнительного Комитета. Положение о государственных трудовых сберегательных кассах Союза Советских Социалистических Республик. 27.11.1925 г. // Распубликовано в № 278 Известий ЦИК Союза ССР и ВЦИК от 05.12. 1925 г.

банковской тайны, подчеркивая равные права на конфиденциальность и для индивидуальных лиц, и для организаций в финансовом секторе.

Подтверждение наличия гарантий института тайны вклада можно найти в Уставе государственных трудовых сберегательных касс от 1977 года. Ст. 26 декларировала следующее: «справки о счетах организаций и учреждений и о совершаемых по ним операциям могут выдаться этим организациям и учреждениям и их вышестоящим органам, а также судам, органам предварительного следствия, органам дознания и финансовым органам с соблюдением установленного порядка»[393].

Разрушение структур Советского Союза привело к переосмыслению многих аспектов экономической жизни, в том числе к рассмотрению роли банковской тайны в новой экономической реальности. Российское законодательство, отражая изменения времени, оформило концепцию «банковской тайны» в Законе РСФСР от 02.12.1990 № 395-I «О банках и банковской деятельности в РСФСР» (далее – Закон о банках), принятом в 1990 году[394].

В 25-й статье Закона о банках было установлено, что все банки, включая Центральный Банк Российской Федерации (Банк России), несут ответственность за сохранность сведений о счетах и операциях своих клиентов и корреспондентов. Обязательство по соблюдению банковской тайны наложено на весь персонал финансовых учреждений, обеспечивая комплексное подход к охране конфиденциальной информации.

Выдача справок, отражающих движение средств и состояние счетов юридических лиц и других организаций, допускается как самим этим организациям, так и их управляющим структурам, государственным налоговым органам, арбитражным инстанциям, судам, следственным органам, а также аккредитованным аудиторским фирмам. Что касается физических лиц, информация о счетах и вкладах предоставляется не только самим владельцам

---

[393] Постановление Совета Министров СССР, 11 июля 1977 г. Об утверждении Устава Государственных трудовых сберегательных касса СССР // Решения партии и правительства по хозяйственным вопросам: Сб. док. Т. 12. Июль 1977 г. март 1979 г. – М.: Политиздат, 1979.

[394] Закон РСФРС от 02.12.1990 № 395-I «О банках и банковской деятельности в РСФСР» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР от 1990 г., № 27, ст. 357.

счетов и их официальным представителям, но и судебным органам и следователям — при условии, что в рамках делопроизводства может возникнуть необходимость наложения ареста, применения взыскания либо конфискации имущества, размещенного на счетах или во вкладах[395].

В ситуации смерти владельца счета или вклада информация о соответствующих счетах может быть предоставлена лицам, которых он специально упомянул в своем завещательном распоряжении, составленном для банка. Аналогичные сведения передаются государственным нотариальным конторам, ведущим наследственные дела, связанные с вкладами умерших, а также иностранным консульским учреждениям, если вопрос касается наследственных прав иностранных граждан.

Ст. 25 Закона РСФСР просуществовала до 1996 года, когда в нее были внесены изменения. Редакция Закона от 03.02.1996 г. № 17 – ФЗ в ст. 26 сформулировала банковскую тайну следующим образом: «Кредитная организация, Банк России, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону». Положения о справках остались неизменными, что наталкивает нас на мысль о том, что ст. 26 обладает признаками неконституционности.

Как выше описывалось, банковская тайна напрямую связана с нормами Конституции РФ и вытекает из положений ст. 23, которая посвящена неприкосновенности частной жизни, семейной и личной тайне, что в свою очередь корреспондирует со п. 7 ст. 3 Закона об информации[396], а также положениями ст. 6 Закона о персональных данных[397], и в совокупности приводит к мысли о том, что

---

[395] Закон РСФРС от 02.12.1990 № 395-I «О банках и банковской деятельности в РСФСР» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР от 1990 г., № 27, ст. 357.

[396] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

[397] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006. № 165.

установленный в ст. 26 Закона о банках процедура предоставления информации должна быть изменена и у клиента необходимо спрашивать разрешения на предоставление информации о нем.

Сравнивая два определения одной и той же категории, можно прийти к следующим выводам:

– обязанность хранить банковскую тайну существует не только у банков, но и Банка России (хотя его сложно отнести к банкам в классическом понимании);

– само определение стало рамочным. Банк вправе устанавливать иной перечень сведений;

– изменился и расширился перечень субъектов, кому могут быть выданы справки по операциям и счетам (суды, Счетная палата РФ и т. д.);

– предусматривается ответственность за разглашение сведений, составляющих банковскую тайну.

Не стоит забывать, что в 1996 году начала действовать, принятая в 1995 году, вторая часть ГК РФ, которая содержит положение о банковской тайне. Ст. 857 гласит, что банк дает свои гарантии по обеспечению тайны банковского счета и вклада, операций по счету и сведений клиента. Присутствие нескольких одинаковых категорий порождало неопределенность, поэтому Конституционный суд РФ отдельно остановился на данном вопросе в ранее указанном Постановлении и дал возможность судам самостоятельно выбирать главенствующую норму.

Рассмотрев нормативные определения банковской тайны, можно сделать вывод, что существует логическое несоответствие в подходах по определению категории, которое приводит к неопределенному правовому регулированию выражающемся в следующем:

– ГК РФ обязывает обеспечивать банковскую тайну исключительно банк, в свою очередь, Закон о банках использует понятие «кредитная организация», которое шире, чем банк;

– ГК РФ признает в качестве тайных только операции по счету, Закон о банках говорит об операциях в общем;

– ГК РФ включает персональные данные о клиенте в содержание банковской тайны, а Закон о банках нет;

– ГК РФ не говорит о корреспондентах кредитной организации, Закон о банках отдельно выделяет их.

Изучив содержание института банковской тайны, представляется целесообразным совместить исследование с изучением категории в доктрине права.

К.А. Маркелова подчеркивает, что сфера банковской тайны включает в себя любую информацию о клиентах и корреспондентах финансового учреждения и Центрального Банка России, которая стала им доступна в процессе выполнения банковских операций и должна быть надежно защищена согласно действующему законодательству. Помимо этого, к банковской тайне причисляются дополнительные данные, которые финансовое учреждение признает конфиденциальными на основании законодательных актов. Такая информация охраняется как для защиты интересов клиентов, так и для обеспечения безопасности самого финансового учреждения[398].

В работах С.А. Даниленко банковская тайна представлена как комплекс конфиденциальных данных, которые финансовые учреждения накапливают в процессе своей деятельности. Отличительной чертой такой информации является ее значительная важность и ценность для кредитных организаций. Законодательная база накладывает жесткие рамки на распространение этих сведений, строго регламентируя их обращение. Доступ к информации, подпадающей под определение банковской тайны, ограничен, и обнародование ее третьим лицам, не участвующим в деятельности банка и его операциях, запрещено[399].

Анализируя различные трактовки понятия банковской тайны, можно выработать собственное понимание этого термина. *Под банковской тайной предлагается понимать такой вид конфиденциальной информации о клиентах*

---

[398] Маркелова К.А. Банковская тайна: правовые аспекты : дис. … канд. юрид. наук: 12.00.14. Саратов, 2000. С. 8.

[399] Даниленко С.А. Правовое регулирование банковской тайны : автореф. дис. … канд. юрид. наук: 12.00.03. М., 2007. С. 15-16.

банка, который получается и аккумулируется в ходе исполнения банком его профессиональных функций и операций. Этот спектр данных охраняется законом, что обязывает банковские институты обеспечивать их неприкосновенность и не допускать разглашения без согласия клиента или других установленных законом оснований.

В свою очередь, *под правовым режимом банковской тайны, понимается смежный правовой институт обеспечения конфиденциальности информации, представляющий собой совокупность сведений о клиенте кредитной организации.*

Объект правового института нормативно не определен, однако, базируясь на полученных результатах исследования, можно прийти к выводу, что в данных правоотношениях объектом выступает несколько видов тайн (субинститутов института банковской тайны): тайна банковского вклада (депозита), тайна банковского счета, тайна операций по счету, тайна частной жизни клиента.

Можно выделить характерные черты банковской тайны:

– содержание банковской тайны включает в себя тайну сведений о вкладчиках, тайну вкладов, тайну счетов и операций, а также ответственность;

– на протяжении всей истории института был определен перечень субъектов, которым могли быть предоставлены сведения;

– институт банковской тайны отстаивает интересы вкладчика клиента кредитной организации. Стоит отметить, что сущностные характеристики не меняются. Одна и та же информация с позиции клиента будет охраняться институтом банковской тайны, в то время как с позиции банка будет применяться правовой режим коммерческой тайны.

Субъектный состав данных правоотношений можно сформировать следующих образом: 1) кредитная организация; 2) Банк России; 3) клиент; 4) органы и организации, имеющие право на получение информации (суды, органы следствия и так далее). Стоит отметить, что при расширении количества органов, которые имеют право получать доступ к банковской тайне, необходимо соблюдать баланс публичных и частных интересов. Показательным примером в данном вопросе является принятие Федерального закона от 17.02.2021 № 6-ФЗ «О

внесении изменений в часть первую Налогового кодекса Российской Федерации», согласно которому, налоговые органы получили доступ ко всей информации о клиента в банке (включая оттиски печатей и образцы подписей)[400]. Данное положение нарушает права клиентов кредитной организации, передача персональных данных предполагает, по меньшей мере, уведомление клиентов, а также, по сути, сильно ограничивает институт банковской тайны, существование которого предполагается обособленно от налоговых органов.

Разделение банковскую и коммерческую тайны, именно с такой точки зрения на вопрос придерживается российский законодатель, вполне оправдано в силу нескольких причин:

1) тайны отличаются по субъектному составу лиц, устанавливающих объем и содержание (банковская тайна устанавливается федеральным законодателем, коммерческая тайна устанавливается по желанию руководителя);

2) отличаются собственники информации (в банковской тайне владельцем является клиент, в коммерческой тайне владельцем выступает учредители коммерческой организации);

3) различаются основания наступления ответственности (установление и соблюдение режима банковской тайны является обязанностью всех работников банков, за ее неисполнение они несут ответственность, коммерческая тайна устанавливается по желанию организации).

Демонстрируя различия между коммерческий и банковской тайнами, можно предположить, что институт банковской тайны, в некоторых правоотношениях, рассматривается как гарантийный элементы защиты смежных видов тайн (аудиторской, налоговой, коммерческой), он дополняет их, и комплексно они образуют безопасный правовой режим для хозяйствующего субъекта.

Отдельным элементом, образующим правовой режим банковской тайны выступает ответственность в данной сфере, которая, в свою очередь, предоставляет клиентам гарантии осуществления их прав и защиты их интересов.

---

[400] Федеральный закон от 17.02. 2021 № 6-ФЗ «О внесении изменений в часть первую Налогового кодекса Российской Федерации» // Российская газета. 19.02.2021. № 36.

Институт ответственности в данной сфере образуется из норм гражданского, трудового, административного и уголовного законодательства.

Гражданско-правовая ответственность за разглашение банковской тайны воплощается в праве клиента требовать от кредитной организации возмещения причиненного материального и нематериального вреда. Имущественную выгоду получает то лицо, чье право на банковскую тайну было нарушено.

Обсуждение в юридической литературе вопроса о том, кто должен нести ответственность за неправомерное разглашение банковской тайны, указывает на неоднозначность этой темы. Согласно п. 3 ст. 857 Гражданского кодекса РФ, ответственность за подобные действия может быть возложена на саму кредитную организацию. Исходя из этого, можно выделить несколько ключевых моментов:

1. Имущественная ответственность ложится на плечи банка, а не на отдельно взятых сотрудников банка.

2. Банк может быть привлечен к ответственности исключительно по инициативе клиента, подавшего соответствующее заявление.

3. Клиент вправе требовать возмещения полного объема ущерба, как это предусмотрено законом, включая не только фактический ущерб, но и упущенную выгоду.

Кроме того, п. 9 ст. 26 Федерального закона «О банках и банковской деятельности»[401] дополнительно расширяет круг лиц, которые могут быть привлечены к ответственности за разглашение сведений, составляющих банковскую тайну. В нем акцент смещается с прав клиента на получение компенсации на обязанности субъектов, ответственных за сохранность банковской тайны. Таким образом, фокусируется внимание не только на правах пострадавших клиентов, в случае утечки конфиденциальной информации, но и на непосредственных обязанностях и ответственности самих банковских учреждений и их работников.

---

[401] Федеральный закон от 02.12.1990 № 395–1 «О банках и банковской деятельности» // Собрание законодательства РФ. 05.02.1996. № 6. Ст. 492. (В данном виде документ опубликован не был. Первоначальный вариант текста документа опубликован в приведенном источнике).

Также предоставляется возможность требования от банка выплаты неустойки по ст. 330 ГК РФ. Однако имеющиеся юридические гарантии не снимают вопрос о том, что работник банка становится носителем информации вне зависимости от его собственного желания, и при смене места работы может нанести вред клиенту кредитной организации, в таком случае, процесс привлечения лица к ответственности будет осложнен, что в свою очередь, может привести к гораздо более существенному вреду чем, если бы лицо оставалось сотрудником банка.

Внедрение законодательных актов, обеспечивающих сохранение конфиденциальности информации после ухода сотрудника с места работы, представляется сегодня крайне необходимым. Важность таких мер обусловлена потребностью в непрерывной защите чувствительных данных, в том числе и банковской тайны. Кроме того, клиенты должны иметь законное право на информирование о запросах, связанных с их личными сведениями, предоставленными банкам. Это будет способствовать большей прозрачности и доверию со стороны клиентов к финансовым учреждениям.

Однако стоит учесть исключения, при которых такое информирование не проводится, например, в рамках специальных операций, осуществляемых в процессе расследования уголовных дел, чтобы не мешать правоохранительной деятельности. Такие меры позволят укрепить правовую защиту конфиденциальной информации и дадут клиентам более четкое понимание уровня их юридической защиты.

Основой для наступления дисциплинарной ответственности служит наличие трудовых отношений между банком и его сотрудником. Согласно нормам Трудового кодекса Российской Федерации, работник несет ответственность за несанкционированное раскрытие информации, признаваемой законом в качестве тайны (конфиденциальной, служебной, профессиональной и других видов). Согласно ст. 57 ТК РФ, трудовое соглашение между сотрудником и финансовым учреждением может включать специальные условия, в числе которых —

требование о неразглашении данных, составляющих объект охраны законодательства.

В случае нарушения этого условия и допущения утечки информации имеет место основание для расторжения трудового договора со сотрудником в соответствии с пп. «в» п. 6 ч.1 ст. 81 ТК РФ. Таким образом, дисциплинарная ответственность применяется непосредственно в отношении того работника, который нарушил условия конфиденциальности, обозначенные в трудовом договоре.

Судебная практика сформировала подход, согласно которому работодатель должен доказать, что работник должен быть сохранять режим конфиденциальности, а также, что массив информации охраняется законом и они стали известны лицу в силу выполнения трудовых обязанностей[402]. Также работник, в соответствии со п. 7 ч. 1 ст. 243 ТК РФ, может быть привлечен к полной материальной ответственности.

Уголовно-правовая ответственность предусмотрена ст. 183 УК РФ, данный состав преступления является единым для преступлений в сфере коммерческой, банковской и налоговой тайны.

Административно-правовая ответственность в данной сфере регулируется ст. 13.14 КоАП РФ. Изучив содержание юридической нормы, можно сделать вывод о том, что банковские работники могут быть привлечены к административной ответственности только в том случае, если за данные деяния не предусматривается уголовно-правовое наказание.

Рассмотрение аспектов административно-правовой ответственности за нарушение норм по обработке персональных данных необходимо осуществлять с учетом положений статьи 13.11 Кодекса об административных правонарушениях РФ. Данная статья устанавливает ответственность за несоблюдение законодательства при выполнении операций с личными данными граждан, что

[402]Решение Дорогомиловского районного суда г. Москвы от 08.02.2021 по делу № 2–304/21. URL: https://mos-gorsud.ru/rs/dorogomilovskij/services/cases/civil/details/03c2ba0f-799c-4920-af7e-84ead7d89958 (дата обращения: 25.07.2025).

включает неправомерный сбор, хранение, использование или распространение такой информации.

Ответственность по этой статье не ограничивается только работниками кредитных организаций. Круг ответственных субъектов расширяется до включения Центрального банка Российской Федерации, аудиторских компаний, а также других специализированных организаций, в том числе и институтов, занимающихся борьбой с легализацией (отмыванием) доходов, полученных преступным путем. Сотрудники этих организаций также могут быть привлечены к ответственности за аналогичные правонарушения.

Процесс привлечения к административной ответственности для вышеупомянутых лиц регламентируется теми же правилами, что и для сотрудников банков. Это обеспечивает единообразие подходов и равенство всех субъектов перед законом, ограничивая возможность злоупотреблений и нарушений при обработке персональных данных граждан.

В качестве проблемы можно выделить неопределенность круга лиц, имеющих полномочия требовать раскрытия банковской тайны в отношении организаций. При этом невыполнение требований государственного органа банком влечет возможность привлечения кредитной организации к административной ответственности по ч. 5. ст. 19.8. КоАП РФ.

По мнению Автора, является неверным тот факт, что законодатель не ввел в основные понятия, которые используются в Федеральном законе, определение банковской деятельности, тем самым, не дав возможности правоприменителям устанавливать ее признаки и впоследствии отграничивать данную деятельность от смежных с ней видов деятельности, например предпринимательской.

В силу того, что банковская тайна регулируется различными нормативными правовыми актами, правоприменитель должен четко определить метод правового регулирования и в точности определить правоотношение, в котором возникло правонарушение.

Проблема определения начала правоотношений между банком и клиентом заключается в том, что существующие нормы законодательства не всегда четко

указывают этот момент. Согласно Закону о банках, статье 26, охрана банковских данных предоставляется для информации, связанной с проведением операций, счетами и вкладами. Возникают ситуации, когда банк уже обладает персональными данными потенциального клиента до официального оформления отношений, например, в процессе анализа кредитоспособности, что ставит под вопрос момент возникновения банковской тайны.

Чтобы устранить этот правовой пробел, можно предложить дополнить ст. 1 соответствующего закона определением «клиент банка», включив в него лиц, предоставивших банку необходимую информацию для начала банковского обслуживания. Это поможет задать четкие рамки договорных отношений.

Однако одних дефиниций недостаточно, поскольку между статьей 26 Закона о баках и статьей 857 Гражданского кодекса РФ существует несоответствие в определении того, какие сведения подлежат защите в рамках «банковской тайны». Это приводит к правовой неопределенности относительно объема защищаемой информации и требует уточнения и гармонизации норм в двух документах.

К тому же ведение перечня конфиденциальной информации оставлено на усмотрение банка, что может вызвать риски по определению охраняемых сведений как банковской тайны, и необходимо более четко закрепить эти критерии на законодательном уровне.

Также существуют риски по идентификации клиента, данная тема должна решаться в комплексе с обозначенными проблемами, чтобы обеспечить надежную правовую защиту интересов как клиентов, так и банковских учреждений.

Правовой режим налоговой тайны

Осуществление экономической деятельности корреспондируется с контролем со стороны государства, это оправданно с точки зрения экономической безопасности государства и стабильности функционирования финансовой системы страны в целом, налоговые органы играют ключевую роль в процессе аккумулирования денежных средств.

Крайне остро стоит вопрос о регулировании налоговой тайны, особенно в свете усиления позиций налоговых органов, часть данного процесса упоминалась ранее в работе. Сформировалась тенденция в большинстве стран мира о необходимости раскрытия налоговой информации для повышения транспарентности в налоговом администрировании. Данная идея прослеживается в Соглашении компетентных органов об автоматическом обмене финансовой информацией от 29.10.2014[403]. Данное соглашения расширило объем данных, которые хранятся в массивах данных налоговых органов РФ.

Институт налоговой тайны испытал существенные изменения вследствие ратификации Российской Федерацией Конвенции о взаимной административной помощи по налоговым делам (далее- Конвенция). Этот международный документ получил статус закона на территории России в соответствии с Федеральным законом от 4 ноября 2014 года № 325-ФЗ[404]. Конвенция, являющаяся результатом совместных усилий стран-участниц, нацелена на укрепление прозрачности налоговой системы и эффективности борьбы с налоговыми злоупотреблениями на международном уровне.

Это соглашение представляет собой новаторское явление в сфере международного налогового регулирования, поскольку оно облегчает обмен информацией между странами в налоговых вопросах. Принятие данной Конвенции сигнализирует о переходе к новому уровню взаимодействия между налоговыми органами различных государств и о готовности к более тесному сотрудничеству по предупреждению и разоблачению налоговых преступлений, а также к совместной работе по обеспечению соблюдения налогового законодательства.

Формирование подобных основ гарантирует эволюцию механизма межстранового обмена сведениями, составляющими налоговую тайну.

Увеличение количества данных, которыми управляют налоговые службы, подчеркивает необходимость нахождения баланса между интересами общества и

---

[403] Россия получила доступ к информации о счетах своих граждан в 80 странах. URL: https://www.nalog.ru/rn78/news/smi/6068722/ (дата обращения: 02.03.2025).

[404] Федеральный закон от 04.11.2014 № 325-ФЗ «О ратификации Конвенции о взаимной административной помощи по налоговым делам» // Российская газета. 07.11.2014. № 254.

правами личности. В частности, это касается обеспечения конфиденциальности хранимых данных. Охрана информации становится ключевым фактор в укреплении имиджа налоговой службы и доверия граждан ведь данные, которые налоговые органы получают от налогоплательщиков, передаются им добровольно или являются обязательными к предоставлению в соответствии со ст. 23 и 80 Налогового кодекса РФ и включают в себя информацию от третьих лиц, таких как банки и иные налоговые агенты.

Эти сведения – плод ежедневной работы налоговых инспекций. Задача этих учреждений не только в сборе и анализе данных, но и в их защите, поскольку они являются конфиденциальными и составляют налоговую тайну. Это включает в себя регистрацию налогоплательщиков, прием и проверку налоговых деклараций, учет взаиморасчетов с бюджетом, а также иные процедуры, которые связаны с обработкой налоговой информации. Гарантирование безопасности этого процесса является фундаментальной обязанностью налоговых органов в контексте охраны прав налогоплательщиков и поддержания целостности фискальной системы страны[405].

Налоговые органы получают не только информацию, которая связана непосредственно с налогами, но и сведения составляющие семейную и личную тайну, охрана которых гарантируется государством[406]. На данном этапе происходит трансформация правового режима охраны сведений.

Развитие цифровой экономики подразумевает активное внедрение и использование электронного документооборота в коммерческой и государственной деятельности.

В качестве пионера в области информатизации органов государственной власти выступает Федеральная налоговая служба (ФНС России), которая успешно реализовала систему личных кабинетов налогоплательщиков, предназначенных для различных категорий пользователей: физических лиц, индивидуальных

[405] Кучеров И.И., Торшин А.В. Налоговозначимая информация в составе охраняемой экономической информации // Финансовое право. 2001. № 1. С. 25.

[406] Налоговое право. Общая часть: в 2 т. Т. 2: учебник и практикум для академ. бакалавриата / под ред. И.И. Кучерова. М.: Юрайт, 2016. 543 с.

предпринимателей и юридических лиц. Эти кабинеты упрощают процедуру электронного документооборота, оптимизируют взаимодействие между налоговой и налогоплательщиками, а также способствуют оперативному доступу к налоговой информации.

Однако с ростом электронного обмена данными, важно должным образом защищать персональная информация и обеспечивать конфиденциальность персональных данных. Законодательное определение налоговой тайны, как системы обеспечения конфиденциальности, зафиксировано в статье 102 Налогового кодекса Российской Федерации.

Кроме того, значительный вклад в разработку теоретических основ защиты информации внесли такие известные ученые-правоведы, как И.И. Кучеров и А.В. Торшин, работы которых призваны дать понимание сложных аспектов охраны информации в контексте налоговых отношений и механизмов ее реализации в условиях цифровизации экономики[407].

Однако наличие подобных категорий не сформировало единого подхода. В частности, статья 102 НК РФ перечисляет виды информации, но, как мы ранее отмечали, данный подход является тупиковый. Понимание категории правового режима налоговой тайны можно сформулировать как совокупность законодательных норм в области налогообложения, устанавливающих принципы защиты конфиденциальности информации о налогах. Эти нормы определяют ограниченный доступ к данной информации, устанавливают процедуры ее обработки, раскрытия и передачи, а также предусматривают ответственность за ее несанкционированное разглашение.

Отсутствие единой практики в данной вопросе способствует возникновению спорных ситуаций.

НК РФ понимает под налоговой тайной всевозможные сведения о налогоплательщике, за исключением сведений из подп. 1-13 п. 1. ст. 102 НК РФ. Сведения возможно представить на материальных или на электронных носителях.

---

[407] Кучеров И.И., Торшин А.В. Налоговая тайна: правовой режим защиты информации. М.: Центр «ЮрИнфоР». 2003. С. 30-31.

Содержание налоговой тайны может включать в себя не только сведения, связанные с налогообложением, а также сведения, составляющие коммерческую, банковскую тайны, персональные данные и т. д. Данное положение говорит о междисциплинарном характере правового института.

Можно сделать вывод о том, что *под налоговой тайной понимается конфиденциальная информация о налогоплательщике или ином лице, которая стала известна органам государственной власти, их должностным лицам, а также иным лицам, которые осуществляли свои права или обязанности, предусмотренных налоговым законодательством.*

Право на налоговую тайну регламентировано положением пп. 13 п. 1. ст. 21 НК РФ. Данное право корреспондирует обязанность налоговых органов обеспечивать соблюдение налоговой тайны, а также сохранность сведений налогообложения, согласно положениям статьи 102 Налогового кодекса РФ, хотя из этого правила существуют исключения. Например, налоговая служба может располагать информацией о лице, которое еще не зарегистрировано в реестре, но уже обладает конфиденциальной информацией, имеющей значение для этого лица. Так, информация о заболеваниях близких родственников, предоставляемая для целей налогового вычета в форме 3-НДФЛ, становится примером данных, защищаемых налоговой тайной вне зависимости от учетного статуса владельца информации. Практика указывает на необходимость охраны конфиденциальных сведений с момента их поступления в налоговую службу, не ожидая регистрации лица.

Такой подход направлен на непрерывную защиту информации и избавление от ограничений, связанных с регистрационными процедурами. В связи с этим, представляется целесообразным рассмотреть возможность исключения из НК РФ п. 9 ст. 84, поскольку временные ограничения ослабляют защиту данных, полученных до момента постановки на учет, а также информации о лицах, зарегистрированных в других налоговых органах.

Налоговая тайна может охватывать разнообразные сведения, зафиксированные в различных формах, будь то документация, электронные файлы,

изображения и так далее, доставленные как на физических носителях, так и посредством сети Интернет. Субъекты, передающие эти сведения, не влияют на их режим как на налоговую тайну.

Сбор информации налоговыми органами происходит в рамках действующих налоговых правоотношений, имеющих нормативный, императивный характер. Органы налогообложения вправе требовать предоставления информации от налогоплательщика в соответствии со статьями 23 и 31 НК РФ. Обязателен учет заложенной в статьях 126 и 129 НК РФ ответственности за нарушение требований по предоставлению данных и соблюдению их конфиденциальности.

Однако любое действие налоговых органов, перечисленное в п. 1 ст. 82 НК РФ, сводится к получению сведений, составляющих налоговую тайну.

В силу крайне широкого подхода к определению изучаемой категории, перечень сведений, составляющих налоговую тайну, является открытым, среди подобных сведений можно сгруппировать и выделить информацию:

– информация о финансово-хозяйственной деятельности: о содержании договоров, о доходах и объемах реализации товаров, работ, услуг, об имуществе и т. п.;

– информация о структуре организации: о персонале, об организационной структуре, функциях подразделениях.

Следует принимать во внимание, что в распоряжении налоговых органов находится информация, не ограниченная только вопросами налогообложения и не регулируемая положениями Налогового кодекса РФ. К числу таких сведений относится информация, связанная с государственной регистрацией юридических лиц и индивидуальных предпринимателей, осуществление которой возложено на налоговые органы в соответствии с постановлением Правительства Российской Федерации.[408]. Данные сведения являются общедоступными, однако, они содержат в себе ряд конфиденциальных сведений, поэтому представляется актуальным сформировать ряд исключений из данного подхода.

[408] Постановление Правительства РФ от 30.09.2004 № 506 (ред. от 28.01.2021) «Об утверждении Положения о Федеральной налоговой службе» // Российская газета. 06.10.2004. № 506.

Следовательно, можно сделать вывод о том, что налоговые органы располагают сведениями, на которые не распространяется режим налоговой тайны, но данные сведения могут носить конфиденциальный характер, соответственно, налоговые органы должны обеспечить сохранность таких сведений.

Сформулировав определение налоговой тайны, необходимо сформулировать определение правового режима налоговой тайны.

Под правовым режимом налоговой тайны предлагается понимать совокупность правовых норм, которые обеспечивают конфиденциальность сведений о налогоплательщике, образующих налоговую тайну.

Объектом данного правового режиме, как мы выяснили выше, является любая информация о налогоплательщике.

Субъектный состав можно условно разделить на две группы:

– лица, обладающие правом на налоговую тайну (налогоплательщики, налоговые агенты);

– лица, обязанные соблюдать налоговую тайну (органы государственной власти – налоговые органы, органы следствия, и т. д., их должностные лица, третьи лица).

Запрет на разглашение сведений, составляющих налоговую тайну, декларирован в п. 2 ст. 102 НК РФ. Данный запрет распространяется на субъектов из п. 1 ст. 102 НК РФ, их должностных лиц, а также на привлекаемыми этими субъектами экспертов и переводчиков. Некоторые ученые расширяют перечень обязанных лиц, включая в него свидетелей, понятых[409]. Данная точка зрения представляется оправданной.

Для хранения и доступа к информации, составляющей налоговую тайну, предусмотрен особый порядок, закрепленный в п. 3 ст. 102 НК РФ.

В данном правовом институте также прослеживается специфика, которая выражается в трансформации правового режима защиты информации. Сущностное наполнение остается прежним, меняется лишь инструментарий защиты. Также, в

[409] Костенко М.Ю. Правовые проблемы налоговой тайны : дис. … канд. юрид. наук: 12.00.14. М., 2002. 146 с.

качестве отличительной особенности налоговой тайны, можно выделить то обстоятельство, что налоговая тайна, в отношении коммерческих организаций, носит характер не только производный, как описывалось раньше, но первостепенный характер, так как коммерческие организации регистрируются в органах ФНС России. Следовательно, до регистрации распространить институт защиты на сведения крайне проблематично, и только после регистрации возникает эвентуальность применять правовой инструментарий защиты (режим коммерческой, налоговой тайны).

Для полного рассмотрения правового института необходимо обратиться к установленной российским законодательством ответственности в данной сфере. За нарушение правового режима налоговой тайны субъекты могут быть привлечены к гражданско-правовой, административной, уголовной ответственности.

Гражданско-правовая ответственность предусматривается положениями ст. 35 НК РФ. Данная норма гарантирует возмещение, причиненных налогоплательщикам убытков вследствие неправомерных действий (бездействий) налоговых органов, должностных лиц, других работников указанных органов при осуществлении ими служебных полномочий за счет федерального бюджета.

Уголовно-правовая ответственность предусмотрена ст. 183 УК РФ, данный состав преступления является единым для преступлений в сфере коммерческой, банковской и налоговой тайны.

Кроме названного состава преступления должностное лицо может быть привлечено к ответственности по ст. 293 УК РФ – «Халатность». Под халатностью понимается неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей, повлекшее причинение крупного ущерба. Такое неисполнение может повлечь выход документов, содержащих сведения, составляющих налоговую тайну, из владения соответствующего органа или лица, в том числе и их уничтожение[410].

[410] Крохина Ю.А. Правовой режим защиты налоговой информации и вопросы его оптимизации // Налоги и финансы. 2015. № 3 (27). С. 40-45.

Стоит отметить тот факт, что несмотря на схожесть по характеру налоговой и коммерческой тайны, правовой режим налоговой тайны отличен от коммерческой и банковской, следовательно, вызывает сомнение факт целесообразности включения в ст. 183 УК РФ норм, связанных с налоговой тайной. Представляется более логичным включение данной нормы в главу 30 X раздела «Преступления против государственной власти», с формирование отдельного состава.

Административно-правовая ответственность в данной сфере регулируется ст. 13.14 КоАП РФ. Изучив содержание юридической нормы, можно сделать вывод о том, что банковские работники могут быть привлечены к административной ответственности только в том случае, если за данные деяния не предусматривает уголовно-правовое наказание.

Глубокое понимание административно-правовой ответственности включает в себя изучение массива нормативных правовых актов, в частности статьи 13.11 Кодекса об административных правонарушениях Российской Федерации (КоАП РФ). Данная статья четко определяет юридические последствия для лиц, нарушающих законодательные требования по управлению персональными данными граждан, включая их сбор, хранение, использование и распространение.

Правомерность обработки персональных данных является важным аспектом в практике законодательства о защите прав граждан на конфиденциальность их личной информации. Статья 13.11 КоАП РФ выступает как одна из мер правового регулирования в этой области, налагая административную ответственность за действия или бездействия, которые приводят к нарушению установленного порядка и могут ущемлять права субъектов персональных данных.

В случае несоблюдения требований, установленных в законах, регулирующих обработку персональных данных, виновные лица привлекаются к административной ответственности, что может выражаться как в назначении штрафных санкций, так и в применении иных административных мер. Подобная практика свидетельствует о принципиальной позиции государства в вопросах

обеспечения конфиденциальности информации и соблюдения установленных стандартов обращения с персональными данными.

С учетом специфики, можно выделить комплексный публично-правовой институт тайны, который объединяет в себе «субинституты» банковской и налоговой тайны, а также нормы других отраслей права, следовательно, возникает вопрос о правовых границах, охватываемых институтом налоговой и иных видов тайн.

У законодателя есть важное упущение в вопросе передачи информации – механизм защиты трансформируется. Данное обстоятельство требует четкой согласованности. Упущение – в соответствии с п. 3 ч. 1 ст. 102 НК РФ режим налоговой тайны не распространяется на сведения о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения.

Еще одним упущением является размытая формулировка разглашения, закрепленная в НК РФ. Данное определение не полное, суть в том, что круг сведений, образующих налоговую тайну, гораздо шире и включает не только сведения, составляющие производственную и коммерческую тайну, но и другие сведения о налогоплательщике, включая персональные данные[411].

Устранение юридических противоречий, возникающих в вопросах конфиденциальности, может быть достигнуто путем введения специализированного нормативного правового акта.

Такой документ предложил бы четкие определения и рамки для различных типов профессиональных тайн, включая стандарты для классификации информации по уровням конфиденциальности. Он мог бы включать в себя принципы конфиденциального обращения с информацией, критерии для определения различных видов тайн, а также явные разграничения режимов конфиденциальности в зависимости от содержания информации.

Также важным стало бы описание основных элементов каждого режима конфиденциальности и, что критически важны обоснования для введения

[411] Данная позиция подтверждается судебной практикой. Решение Арбитражного суда Приморского края от 24.09.2024 по делу № А51-15065/2024 //СПС «КонсультантПлюс».

наказаний за нарушение конфиденциальности информации. Это позволило бы не только предоставить юридически четкий водораздел между различными категориями сведений и их уровнем тайности, но и укрепило бы правовые механизмы защиты от неправомерного раскрытия данных.

Такой подход помог бы устранить неоднозначности и давал бы четкие руководства для органов власти, корпоративных субъектов, профессионалов различных отраслей и граждан, касающихся использования и защиты конфиденциальной информации в профессиональной деятельности, способствовал бы повышению уровня правовой защищенности субъектов данных и ответственного обращения с ними.

Совершенствование правового регулирование частично можно осуществить через установление специальных экспериментальных правовых режимов для апробации новых подходов к работе с информацией.

Существует несколько принципиальных направлений для правовой регуляции информации, подлежащей защите в рамках различных видов тайн. Эти подходы оформлены в действующем законодательстве и применяются в различных ситуациях:

1. Перечисление в нормативном акте: в этом случае важные сведения, требующие конфиденциальности, точно и исчерпывающе перечисляются в нормативных правовых актах. Такой метод предоставляет четкую законодательную базу для определения тайны и обеспечивает ясность в вопросах ответственности за ее разглашение.

2. Определение собственником информации: здесь отдельные лица или организации, являющиеся обладателями конфиденциальной информации, имеют право самостоятельно устанавливать, какие сведения они считают защищаемыми. Такой подход предоставляет гибкость в управлении собственной информацией и позволяет адаптировать охрану данных под индивидуальные нужды.

3. Определение ответственных лиц: вместо того, чтобы составлять перечень защищаемых сведений, законодательство определяет круг лиц, обязанных хранить в тайне определенную информацию. Этот метод устанавливает

обязательство о сохранении конфиденциальности для тех, кто, по роду своей деятельности, имеет доступ к «чувствительным» данным.

Каждый из этих подходов имеет свои преимущества и недостатки, и выбор способа зависит от целей защиты информации и конкретного контекста ее использования. Возможно, для более эффективной защиты конфиденциальной информации будет целесообразным сочетание вышеуказанных подходов в рамках комплексной правовой политики[412].

Для восполнения обозначенных пробелов рекомендуется изменить подход к тайнам с учетом реалий. Государству необходимо уступить право основного регулятора тем субъектам, которые образуют режимы тайн.

Современные тенденции в управлении налоговой информацией подразумевают изменение подходов к конфиденциальности налоговых данных. Одной из причин этого служит упрощение процедур доступа к информации через электронные сервисы, такие как личный кабинет налогоплательщика. Вместо жесткого подхода к сохранению налоговой тайны, предлагается разработка более адаптивной модели.

Эта гибкая модель предоставления налоговой информации будет базироваться на принципе индивидуального согласия налогоплательщика. Суть подхода в том, что каждый налогоплательщик может предоставить согласие на раскрытие своих налоговых сведений. Это согласие направляется в Федеральную налоговую службу России (ФНС России) и оформляется в строгом соответствии с формой, форматом и порядком, утвержденным данным ведомством.

Таким образом, налогоплательщик получает возможность самостоятельно контролировать объем раскрываемой им информации, не принимая на себя обязательства по открытию данных. Это соответствует задаче обеспечения общественно значимых целей, какими являются прозрачность и доступность информации, и при этом исключает излишнее ограничение личных прав. Дополнительный механизм контроля за обработкой данных в такой конструкции

---

[412] См. ст. 35 Налогового кодекса Российской Федерации // Российская газета. 06.08.1998 г. № 148-149.

избыточен, поскольку основа модели – добровольное согласие налогоплательщика и его возможность определения рамок раскрытия сведений.

Резюмируя рассмотренные области, можно прийти к выводу, что подход к институтам тайн нуждается в пересмотре, так как с развитием технологий сужается сфера приватности, появляется новая общественная ценность – приватность жизни. Ежесекундно мобильный телефон, роутер, «умный» телевизор, собирают и передают информацию о субъектах.

Связующей проблемой в плоскости является проблема идентификации субъектов.

Сама категория «идентификация» применяется в различных областях жизни. «Идентификация» имеет латинские корни, происходит от «idem» и означает «тот же самый»[413]. «Идентичность» и «идентификация» часто используются в разных науках, что говорит о множественности подходов к ним, в том числе, онтологическом, психологическом, социологическом[414]. Понятие «идентификации» носит междисциплинарный характер.

Развитие законодательства России в области установления личности и подтверждения полномочий личности проходит значительный путь, который начинается с ключевых нормативных правовых актов в начале 2010-х годов. Стартовая точка в этой области отмечается постановлением Правительства РФ от 28.11.2011 года № 977[415], которое заложило фундамент для создания интегрированных систем идентификации и аутентификации.

Данный документ утвердил стандарты для Федеральной государственной информационной системы, известной как «Единая система идентификации и аутентификации». Эта система предназначена для упрощения взаимодействия

---

[413] Латино-русский словарь: 16 000 слов / сост. Д.И. Фомицкий; авторы современной редакции словаря: Л.Ф. Цымлова, Т.А. Ширяева. Ростов-на-Дону: Феникс, 2001. С. 226.

[414] Косенчук Л.Ф. Сущность идентичности и основные подходы к ее исследованию // Теория и практика общественного развития. 2014. № 16. С. 223-225; Лысак И.В. Формирование персональной идентичности в условиях сетевой культуры: монография / Лысак И.В., Косенчук Л.Ф. М.: Изд-во «Спутник+», 2016. 147 с.

[415] Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-техническое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Собрание законодательства Российской Федерации. 2011. №49 (часть V). Ст. 7284.

пользователей с информационными системами государственных и муниципальных услуг, предоставляемых в цифровом формате, и стала краеугольным камнем в структуре электронного правительства России.

Стоит отметить, что правовое регулирование в данной сфере носит фрагментарный характер, не существует единой иерархии терминологии[416] и единых требований к субъектам правоотношений, обладающих организационно-техническими возможностями по идентификации участников правоотношений в Интернете.

Процесс установления личности в виртуальном пространстве значительно отличается от аналогичного процесса в реальной жизни. В Интернете, особенностью является активное участие информационных посредников, обладающих необходимой технологической базой и инфраструктурой. Именно они создают условия для так называемой «относительной идентификации», когда личность пользователя удостоверяется в рамках определенной системы или платформы.

С этим связаны определенные трудности, в том числе вопросы ответственности самих посредников и установление границ в отношении предоставления личных данных клиентов или пользователей. Концепция «абсолютной идентификации», когда личные данные делают человека узнаваемым во многих контекстах и для множества сторонних лиц, вызывает дополнительные опасения по поводу конфиденциальности и безопасности данных.

Прежде чем были внесены изменения постановлением Правительства № 977[417], были закреплены «Требования к ЕСИА». Они положили начало формированию правовых и технологических аспектов идентификации в электронной форме посредством создания «Единой системы идентификации и аутентификации». Эта система является ключевым элементом инфраструктуры для

---

[416] Наумов В.Б. Вопросы развития терминологии в сфере персональных данных // Понятийный аппарат информационного права. Сб. науч. работ / Отв. ред. И.Л. Бачило, Э.В. Талапина. М., 2015. С. 124–129.

[417] Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-техническое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Собрание законодательства Российской Федерации. 2011. №49 (часть V). Ст. 7284.

взаимодействия информационных систем, применяемых для предоставления государственных и муниципальных услуг в цифровой среде.

«Требования к ЕСИА» установили определения, ставшие основой правового процесса идентификации:

1. Идентификация участников информационного обмена требует сверки введенного пользователем идентификатора с данными в базовых государственных информационных ресурсах, что предусмотрено регулятивными актами.

2. Аутентификация является процессом проверки принадлежности введенного идентификатора данному пользователю, а также подтверждением его достоверности.

3. Авторизация представляет собой процедуру, подтверждающую права пользователя на доступ к определенной информационно-технической инфраструктуре и предоставление услуг в электронном виде.

Эти положения являются фундаментальными для функционирования системы, обеспечивающей безопасность и регулирование взаимодействия пользователей и информационных систем в сфере предоставления государственных услуг в России.

В настоящий момент эти определения, наряду с терминами из других отраслей законодательства, в первую очередь финансового[418], и из ряда стандартов[419], представляют собой ограниченную терминологическую базу,

---

[418] Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда» // Собрание законодательства Российской Федерации. 2013. № 52. (ч. 1). Ст. 6991; Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // Собрание законодательства Российской Федерации. 2001. № 33. (ч. 1-2). Ст. 3418; Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1. (ч. 1). Ст. 19.

[419] ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (утв. и введен постановлением Госстандарта России от 09.02.1995 г. №. 49); ГОСТ Р ИСО/ТО 13569-2007. «Финансовые услуги. Рекомендации по информационной безопасности» // (утв. и введен приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2007 г. № 514-ст); ГОСТ Р ИСО/МЭКТО 19791-2008. Национальный стандарт Российской Федерации. «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем». (утв. и введен приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 г. № 525-ст); ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утв. и введен приказом Федерального агентства по техническому регулированию и метрологии от 01.12.2011 г. № 683-ст).

которая нуждается в оперативном развитии.

Без создания четко структурированной системы определений законодательная база может столкнуться с риском хаотического развития. Такой процесс подразумевает внесение специфических дефиниций, формируемых непосредственно под давлением текущих ситуаций и нужд. Однако такие определения часто вступают в противоречие с уже утвержденными и принятыми понятиями, что ведет к расхождениям и конфликтам в правоприменительной практике. Важно стремиться к гармонизации и систематизации законодательства, чтобы исключить возможность таких противоречий.

Современное продвижение цифровой экономики сопряжено с возникновением новых рисков и вызовов, оказывающих влияние на процесс цифровизации. Особое значение в этом контексте приобретает вопрос защиты фундаментальных прав личности в цифровом пространстве — от обеспечения точной идентификации человека с помощью технологий, соответствия цифрового профиля реальному субъекту, до гарантии сохранности пользовательских информационных ресурсов и формирования доверия общества к цифровым платформам.

В рамках обозначенных приоритетов была поставлена цель, изложенная в пункте 1.1 Программы, посвященная необходимости разработки правовых механизмов, способствующих появлению единого пространства доверия в цифровой среде. Уточнение и развитие этого направления отражено в паспорте проекта национальной программы «Цифровая экономика Российской Федерации», где в составе федерального проекта «Нормативное регулирование цифровой среды» (раздел 4.1) появилось дополнительное положение, напрямую касающееся вопросов идентификации. Отмечается, что требуется правовое регулирование особенностей обращения персональных данных, которые массово используются и аккумулируются для целей установления личности.

Существуют конкретные ориентиры: необходимо создать нормативную основу, обеспечивающую безопасный сбор, надежное хранение и корректную обработку информации с применением новых информационных технологий. В

частности, речь идет о формировании порядка обезличивания персональных сведений, определении процедур и условий работы с такими данными, уточнении ответственности за их несоблюдение, а также разработке прозрачных правил получения согласия субъектов на обработку их данных (п. 1.3).

На текущий момент существуют технические средства, позволяющие обходить установленный порядок удаленной идентификации. Примером попытки урегулировать подобные вопросы на законодательном уровне является закон, принятый в штате Иллинойс, который касается использования искусственного интеллекта для анализа видеоинтервью[420]. Согласно данному закону, работодатели, запрашивающие видеоинтервью у соискателей, обязаны заранее уведомить их в письменной форме о возможности использования программы с алгоритмами искусственного интеллекта. Работодатели должны разъяснить, каким образом функционирует данная программа, какие параметры она учитывает и как оценивает кандидатов. После получения письменного согласия соискателя работодатели могут приступить к анализу, при этом им запрещено передавать запись третьим сторонам, за исключением тех специалистов или организаций, чьи технологии необходимы для оценки. Кроме того, после завершения обработки информации в течение 30 дней запись должна быть удалена, что направлено на защиту конфиденциальности кандидатов и предотвращение злоупотреблений.

В Российской Федерации начало формирования правового регулирования в области идентификации связано с введением в 1995 году понятия «персональные данные». Это понятие изначально определялось через задачу установления личности конкретного физического лица. Со временем в различных отраслях законодательства стали появляться нормы, уточняющие порядок идентификации и обработки персональных данных.

Одним из значимых шагов в этом направлении стало внесение изменений в пункт 1 статьи 160 Гражданского кодекса РФ, касающегося соблюдения письменной формы сделки. Новая редакция этой нормы предусматривала

[420] The Artificial Intelligence Video Interview Act. [Электронный ресурс] // General Assembly. 2019. URL: https://legiscan.com/IL/bill/HB2557/2019 (дата обращения: 02.03.2025).

использование средств, которые позволяли достоверно установить личность того, кто выразил волю удаленно, что создавало основу для дальнейшего развития цифровых технологий в правовой практике.

Инициированный Центром компетенций в сфере нормативного регулирования цифровой экономики, действующим при Фонде «Сколково», аналитический проект, посвященный определению перечня сведений, составляющих банковскую, телекоммуникационную, медицинскую и иную профессиональную тайну, а также изучению процедур их передачи третьим лицам, был реализован в рамках реализации Плана мероприятий по нормативному регулированию национальной программы развития цифровой экономики РФ. Основная цель проведенной работы заключалась в разработке методологических подходов, обеспечивающих легитимное и безопасное использование конфиденциальной информации в условиях активно расширяющейся цифровизации различных сервисов.

Особое внимание в результате исследования было уделено вопросам анонимизации и возможной последующей деанонимизации личных данных, что приобретает особую актуальность при обработке значительных массивов информации — так называемых больших данных. Для защиты приватности используются целый спектр инструментов: к их числу относятся методы сокрытия информации, внедрение шумовых алгоритмов, перестановка элементов буквенного состава, а также различные способы шифрования и кодирования, позволяющие минимизировать риски несанкционированного доступа.

В Японии применяется концепция «связующих кодов» (codeslinking), которая нашла широкое использование в процессах анонимизации данных. Эта концепция предполагает, что в рамках алгоритмов анонимизации связующие коды, обеспечивающие возможность идентификации личности, подлежат удалению. Такой подход формирует основу для обезличивания информации, что позволяет

значительно повысить уровень защиты персональных данных, а также минимизировать риски их неправомерного использования[421].

Рассмотрев проблему обеспечения идентификации, можно высказать идею о выделении новых принципов:

– принцип добровольности;

– принцип соразмерности (о котором было сказано выше в исследовании);

– принцип конфиденциальности информации.

Идентификация должна привести к конкретному результату – достоверному установлению лица.

С учетом определения термина «идентификация» и на основе анализа принципов можно сделать вывод о необходимости формирования принципа информационной идентификации.

Под принципом информационной идентификации предлагается понимать *необходимость установления юридической принадлежности информации и прав на ее обработку соответствующим субъектам цифровой экономики.* Он должен сочетать в себе следующие условия:

– не должны быть нарушены права и интересы путем разглашения используемой информации и результатов идентификации;

– не должны пострадать права и интересы идентифицирующего, что не стали известны алгоритмы и решения идентификации;

– сохранность в тайне самого факта идентификации.

Использование принципа информационной идентификации служит основой для формирования среды цифрового доверия. Доверие в цифровую эпоху невозможно без верификации участников и прозрачности алгоритмов, с учетом их

---

[421] Исследование по определению состава тайн Итог. — [сайт Сколково]. URL: https://sk.ru/foundation/legal/m/sklegal03/22588/download.aspx. Руководители и соавторы НИР: В.Б. Наумов, В.В. Архипов; исполнители НИР, соавторы: Р.А. Ахобекова, Т.А. Бовсуновская, Я. В. Бутримович, А.В. Грачева, Е.М. Крамм, С.П. Лялькова, В.О. Полыгалов, К.М. Смирнова, Е.В. Тытюк. Объектом исследования выступили законодательство и правоприменительная практика в России, ЕС и входящие в него страны, Великобритании, США, Японии, Сингапуре, Южной Корее, Израиле, ОАЭ и ряде других стран. (дата обращения: 02.03.2025).

сохранности. Принцип информационной идентификации должен применяться только в той сфере, где без него невозможно обойтись. Сферы же, в которых можно обойтись без идентификации, необходимо применять механизмы анонимности по умолчанию. Принцип информационной идентификации отвечает глобальным тенденциям (например, концепции “Privacy by Design”).

ЗАКЛЮЧЕНИЕ

В процессе выполнения данной диссертационной работы была осуществлена комплексная оценка существующей системы информационно-правового регулирования цифровой экономики, а также выработаны рекомендации по модернизации инструментов, направленных на более эффективное управление многоаспектными информационно-правовыми взаимодействиями в цифровой сфере. Итогом исследования стал успешный выход на поставленные задачи.

Кроме того, в ходе анализа предложено авторское определение информационно-правового обеспечения цифровой экономики, которое отражает не только трансформацию традиционных общественных институтов под влиянием цифровизации, но и специфику совершенно новых форм социальных и правовых отношений, возникающих в условиях цифровой эпохи.

Помимо исследования правовой категории, были предложены новые основополагающие идеи, опираясь на которые необходимо выстраивать систему правовых норм, регулирующих отношения по формированию цифровой экономики. По мнению автора, ключевым элементом построения функционирующей информационной инфраструктуры для цифровой экономики (экономики данных[422]) выступает формирование, и реализация основополагающих начал, а именно — дополнение имеющихся правовых принципов новыми принципами правовой интероперабельности, информационной идентификации и другими. Принцип правовой интероперабельности предполагает создание правовых норм с учетом возможности их применения и адаптации различных субъектов при минимальных изменениях и согласовании с уже действующими нормами. Предполагается, что данный принцип пронизывает все регулируемые общественные отношения, а также корреспондирует с другим предложенным принципом — принципом информационной идентификации, который, в свою очередь, является связующим звеном для формирования среды цифрового доверия.

[422] На момент написания работы автор использует действующий понятийно-категориальный аппарат, так как национальный проект «Экономика данных и цифровая трансформация государства» находится на стадии формирования и взгляд уполномоченных органов на данную страту может меняться.

Принцип правовой интероперабельности позволит унифицировать порядок взаимодействия государственных структур и частного сектора, позволит сэкономить правовой ресурс. Данный принцип является основой для построения цифровой модели государственного управления. В свою очередь, принцип информационной идентификации выступает связующим элементом в условиях развития цифровой экономики, внедрение его в экономические процессы позволит упростить взаимодействие с помощью установления юридической принадлежности информации и прав на ее обработку соответствующим субъектам цифровой экономики. В этой связи, требуется совершенствование правовых механизмов по эвентуальности взаимодействия между субъектами.

Осознание данных принципов неминуемо ведет к изменению подходов осуществления экономической деятельности с применением информационных технологиях, в частности, основываясь на данных принципах, можно прийти к идее необходимости разработки единого стандарта для смарт-контрактов (с условиями отступления от алгоритмов при необходимости).

Технологическое развитие предполагает значительное изменение, в том числе расширение, общественных отношений, складывающихся под влиянием информационных технологий. Посредствам применения информационных технологий, появляется и фиксируется ранее неизвестная информация, например, цифровой след, цифровой почерк субъекта, что является основанием для формирования цифровой личности (цифрового профиля) субъекта. Данная информация может применяться к разным сферам жизни.

Развитие новых технологий подталкивает юридическую науку к поиску решений по их интеграции.

В контексте перехода традиционной экономики к цифровой, на первый план, в качестве ценности, выходят персональные данные субъектов, именно они являются основой для компаний новой формации, образующие их экономическую ценность.

На фоне развития цифровой экономики и возрастания интереса к персональным данным, остро стоит вопрос использования цифровых следов

(цифровой тени), а также правового регулирования «цифрового двойника» и «цифровой личности».

Кроме того, в современном мире появились новые сущности, регулирование которых неопределенно.

Для эффективного государственного и частного управления активно внедряется технология искусственного интеллекта, которая позволяет существенно экономить ресурсы. Однако в работе доказано, что развитие технологии искусственного интеллекта должно происходить поэтапно, правовая система должна быть готова, в качестве составляющего элемента для поэтапной интеграции технологии искусственного интеллекта в работе была доказана идея релевантности подхода по рассмотрению технологии искусственного интеллекта как источника повышенной опасности, для баланса интересов публичного и частного секторов предлагается распространить, в качестве условия для работы участников рынка, инструментарий страхования ответственности за ущерб, причиненный системой. Данная позиция позволит более органично вписать технологию в российскую систему права, однако стоит иметь в виду, что при условии появления «сильной» формы искусственного интеллекта потребуются более масштабные изменения.

Учитывая специфику информационного пространства и искусственного интеллекта, а также признание развития искусственного интеллекта как стратегической цели для лидирования государства в работе акцентируется внимание на необходимости принятия концепции регулирования искусственного интеллекта, которая бы установила принципы разработки и применения технологии, сферы его использования.

Для развития правового обеспечения цифровой экономики и персональных данных в работе сформулированы рекомендации по совершенствованию правового регулирования цифрового профиля. Предлагается создание публичного реестра согласий субъекта данных о возможной передаче данных третьим лицам на срочной основе, основанного на технологии блокчейн. При правовой регламентации цифрового профиля необходимо исходить из риск-

ориентированного подхода. Одним из возможных способов совершенствования правового регулирования инфраструктуры цифрового профиля является создание правовой регламентации механизма уведомления заинтересованных лиц о факте профилирования и применяемых методах. Также представляется важным предоставление права на ознакомление и оспаривание результатов профилирования, а объем предоставляемой информации должен быть минимален — без включения «деликатной» информации, обладающей особой значимостью для субъекта.

Ключевым элементом для осуществления деятельности в рамках цифровизации экономики является использование цифровых валют для расчетов, а также придание экономической ценности цифровым активам (токенам). Расчеты с применением цифровых активов, как указывается в диссертационном исследовании, несут ряд рисков для государства и хозяйствующих субъектов, в первую очередь, это осложненный способ защиты интересов субъектов, так как система децентрализованная и учет не ведется государственными органами. Данная специфика предоставляет абсолютную автономию действий участников отношений, в которых государство, не обладает особым статусом, а выступает в качестве одного из равных участников. Потребность государства в регулировании цифровых активов ясна, но для достижения данной цели необходимо уточнение правового режима объектов, которые поддаются регулированию (национальные цифровые валюты), а также использование «мягкой силы» для конкурентоспособности государственного инструмента.

Обоснована позиция необходимости обязывания субъекта, аккумулирующего денежные средства с помощью инвестиционных платформ, информировать инвесторов о реалистичных стратегиях вложения средств с поэтапным предоставлением отчетности. Для достижения должного регулирования необходима разработка и внедрение правового механизма о неразглашении информации до реализации проекта.

Настоящая диссертация может быть полезна для специалистов в сфере информационно-правового обеспечения цифровой экономики своим теоретическим содержанием и практическим рекомендациям.

Дальнейшая разработка темы диссертационного исследования представляется возможной в силу ее обширности и фундаментальной значимости.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Международные документы

1. Конвенция ООН об использовании электронных сообщений в международных договорах (принята 23.11.2005 Резолюцией 60/21 Генеральной Ассамблеи ООН). URL: https://www.un.org/ru/documents/decl_conv/conventions/elect_com.shtml

2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // СПС «КонсультантПлюс» (дата обращения 04.01.2025 г.).

3. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation / GDPR) // Текст перевода официально опубликован не был; текст Регламента на английской языке опубликован в официальном Журнале, № L 119. 04.05.2016. С. 1-88.

4. Директива Европейского парламента и Совета ЕС 2013/40/ЕС от 12.08.2013. Об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД Совета ЕС. Текст не опубликован.

5. Типовой закон ЮНСИТРАЛ об электронных подписях и Руководство по принятию 2001 г. Нью-Йорк: ООН, 2002. URL: https://www.uncitral.org/pdf/russian/texts/electcom/ml-elecsig-r.pdf.

6. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 may 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). [Электронный ресурс]. URL: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng (дата обращения: 22.04.2024 г.).

Нормативные правовые и иные акты Российской Федерации

7. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 25.12.1993. № 237.

8. Гражданский кодекс Российской Федерации. Часть вторая: федеральный закон от 26.01.1996 № 14-ФЗ // Собрание законодательства Российской Федерации. 1996. № 5. Ст. 410.

9. Гражданский кодекс Российской Федерации. Часть четвертая: федеральный закон от 18.12.2006 № 230-ФЗ // Российская газета. 22.12.2006. № 289.

10. Налоговый кодекс Российской Федерации (часть первая): федеральный закон от 31.07.1998 № 146-ФЗ // Российская газета. 06.08.1998. № 148-149.

11. Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ (с изм. и доп., вступ. в силу с 01.03.2025) // Российская газета. 30.12.2004. № 290.

12. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1990. № 27. Ст. 357.

13. Федерального закона «О рынке ценных бумаг» от 22.04.1996 № 39-ФЗ (ред. от 23.05.2025) // Российская газета. 25.04.1996. № 79.

14. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем» // Собрание законодательства Российской Федерации. 2001. № 33 (ч. 1). Ст. 3418.

15. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // Российская газета. 31.12.2002. № 245.

16. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Российская газета. 10.07.2003. № 135.

17. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3283.

18. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006. № 165.

19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165.

20. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации. 2009. № 7. Ст. 776.

21. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Российская газета. 08.04.2011. № 75.

22. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.

23. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // Собрание законодательства Российской Федерации. 2012. № 53 (ч. 1). Ст. 7598.

24. Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда» // Собрание законодательства Российской Федерации. 2013. № 52 (ч. 1). Ст. 6991.

25. Федеральный закон от 12.03.2014 № 35-ФЗ «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета. 14.03.2014. № 59.

26. Федеральный закон от 04.11.2014 № 325-ФЗ «О ратификации Конвенции о взаимной административной помощи по налоговым делам» // Российская газета. 07.11.2014. № 254.

27. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 31.07.2017. № 167.

28. Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о

внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп., вступ. в силу с 15.07.2023) // Собрание законодательства Российской Федерации. 2019. № 31. Ст. 4418.

29. Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 04.08.2023) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

30. Федеральный закон от 20.07.2020 № 211-ФЗ (ред. от 04.08.2023) «О совершении финансовых сделок с использованием финансовой платформы» // Собрание законодательства Российской Федерации. 2020. № 30. Ст. 4737.

31. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Официальный интернет-портал правовой информации (www.pravo.gov.ru), 31.07.2020, ст. 0001202007310024. URL: http://publication.pravo.gov.ru/Document/View/0001202007310024.

32. Федеральный закон от 17.02.2021 № 6-ФЗ «О внесении изменений в часть первую Налогового кодекса Российской Федерации» // Российская газета. 19.02.2021. № 36.

33. Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Собрание законодательства Российской Федерации. 2023. № 1 (ч. 1). Ст. 19.

34. Федеральный закон от 24.07.2023 № 339-ФЗ «О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» // Российская газета. 31.07.2023. № 167.

35. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7077.

36. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

37. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.

38. Постановление Правительства РФ от 02.03.2019 № 234 «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 11. Ст. 1119.

39. Постановление Правительства РФ от 30.09.2004 № 506 (ред. от 28.01.2021) «Об утверждении Положения о Федеральной налоговой службе» // Российская газета. 06.10.2004. № 506.

40. Постановление Правительства РФ от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-техническое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Собрание законодательства Российской Федерации. 2011. № 49 (часть V). Ст. 7284.

41. Постановление Правительства РФ от 03.06.2019 № 710 (ред. от 02.02.2024) «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» (вместе с «Положением о проведении эксперимента…»): электрон. ресурс // Офиц. интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201906070031.

42. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» //

Собрание законодательства Российской Федерации. 2017. № 31. Ст. 4418 (утратило силу).

43. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства Российской Федерации. 2020. № 35. Ст. 5593.

44. Проект Федерального закона № 424632-7 «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации» (ред., внесенная в ГД ФС РФ, текст по состоянию на 26.03.2018). URL: file:///Users/mac/Downloads/424632-7260320184246 32-7.pdf (дата обращения: 05.07.2025).

45. Проект Федерального закона № 419059-7 «О цифровых финансовых активах» (ред., внесенная в ГД ФС РФ, текст по состоянию на 20 марта 2018). URL: http://sozd.parliament.gov.ru/bill/419059-7 (дата обращения: 07.12.2024).

46. Пояснительная записка к проекту Федерального закона № 419059-7: электрон. документ. URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения: 07.12.2024).

47. Письмо ФАС России от 25.09.2019 № АК/83509/19 «О разъяснении по вопросу рекламы в информационно-телекоммуникационной сети Интернет»: электрон. документ. URL: https://fas.gov.ru/documents/ak-83509-19.

48. Положение об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма / утв. Банком России 15.10.2015 № 499-П. (ред. от 20.07.2016). URL: https://sudact.ru/law/polozhenie-ob-identifikatsii-kreditnymi-organizatsiiami-klientov-predstavitelei/.

49. ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. М.: Стандартинформ, 2006. 86 с.

50. ГОСТ Р ИСО/МЭК 20546-2021. Национальный стандарт Российской Федерации. Информационные технологии. Большие данные. Обзор и словарь. М.: Стандартинформ, 2021. 16 с.

51. ГОСТ Р 55602-2012. Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. М.: Стандартинформ, 2012. 10 с.

52. ГОСТ Р ИСО/МЭК 20546-2019. Информационные технологии. Большие данные. Обзор и словарь. М.: Стандартинформ, 2019. 11 с.

53. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. М.: Стандартинформ, 1995. 6 с.

54. ГОСТ Р ИСО/ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности. М.: Стандартинформ, 2007. 62 с.

55. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. М.: Стандартинформ, 2008. 121 с.

56. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. М.: Стандартинформ, 2011. 67 с.

Нормативные правовые и иные акты зарубежных стран

57. Electronic Securities Act (eWpG) (Law of 3 June). URL: https://www.loc.gov/item/global-legal-monitor/2021-06-29/germany-electronic-securities-act-enters-into-force/ (дата обращения: 07.07.2025).

58. Federal Act on the Amendment of the Swiss Civil Code (Part Five: the Code of Obligations) of 30 March 1911 (Federal Act) Government of the Swiss Confederation.

59. Financial Services and Markets Act 2000. URL: https://www.legislation.gov.uk/ukpga/2000/8/contents (дата обращения: 08.07.2025).

60. Jumpstart our business startups act (2012) P.L. 112-106- APR. 5, 2012. URL: https://www.govinfo.gov/content/pkg/PLAW-112publ106/pdf/PLAW-112publ106.pdf (дата обращения: 08.07.2025).

61. Malta National ICT Interoperability Framework. 2019.

62. Securities Act as Amended Through P.L. 115-174, Enacted May 24, 2018. URL: https://www.fsc.go.kr/comm/getFile?srvcId=BBSTY1&upperNo=27272&fileTy=ATTACH&fileNo=2 (дата обращения: 07.07.2025).

63. Securities Exchange Act as Amended Through P.L. 112-158, Approved 10 August 2012. URL: https://www.govinfo.gov/content/pkg/COMPS-1885/pdf/COMPS-1885.pdf (дата обращения: 07.07.2025).

64. The Artificial Intelligence Video Interview Act. [Электронный ресурс] // General Assembly. 2019. URL: https://legiscan.com/IL/bill/HB2557/2019 (дата обращения: 02.03.2025).

65. The California Consumer Privacy Act of 2018. [Электронный ресурс]. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (дата обращения: 23.04.2024).

66. Virtual asset (service providers) Act (2022 Revision) Supplement No. 6 published with Legislation Gazette No. 7 dated 31st January, 2022. URL: https://legislation.gov.ky/cms/images/LEGISLATION/PRINCIPAL/2020/2020-0014/VirtualAssetServiceProvidersAct_2022%20Revision.pdf (дата обращения: 07.07.2025).

67. Закон Штата Аризона № 2417 от 29.03.2017. URL: https://legiscan.com/AZ/text/HB2417/id/1588180 (дата обращения: 07.07.2025).

68. 中华人民共和国电子商务法 № 7 (Закон КНР «Об электронной коммерции» от 31.08.2018). URL: http://www.mofcom.gov.cn/article/zt_dzswf/deptReport/201811/20181102808398.shtml (дата обращения: 23.04.2024).

69. Об информации, информатизации и обеспечении информационной безопасности: Модельный закон (Приложение к Постановлению МПА СНГ от 28.11.2014 № 41-15).

70. Приложение 1 к Декрету Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» в п. 9 перечня используемых терминов и их определений содержит следующую дефиницию смарт-контракта: «программный код, предназначенный для функционирования в реестре блоков транзакций (блокчейне), иной распределенной информационной системе в целях автоматизированного совершения и (или) исполнения сделок либо совершения иных юридически значимых действий». [Электронный ресурс] // Национальный интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0 (дата обращения: 07.07.2025).

71. О проекте европейского закона об управлении данными - Data Governance Act. URL: https://d-russia.ru/o-proekte-evropejskogo-zakona-ob-upravlenii-dannymi-data-governance-act.html (дата обращения: 22.04.2024).

Нормативные правовые акты, имеющие историческое значение

72. Основы гражданского законодательства Союза ССР и республик (утв. ВС СССР 31.05.1991 № 2211-I) // Ведомости СНД и ВС СССР. 1991. № 26. Ст. 733. С. 136.

73. Закон СССР от 26.05.1988 № 8998-XI. О кооперации в СССР // Ведомости Верховного Совета СССР. 1988. № 22. Ст. 355.

74. Закон СССР от 04.06.1990 № 1529-I. О предприятиях в СССР // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР. 1990. № 25. Ст. 460.

75. Закон РСФСР от 02.12.1990 № 395-I. О банках и банковской деятельности в РСФСР // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1990. № 27. Ст. 357.

76. Положение о городских общественных банках (утв. 10.06.1862 г.) // Полное собрание законов Российской империи. Собр. II. Т. XXXVII. № 38362. СПб., 1862. 834 с.

77. Постановление Президиума Центрального Исполнительного Комитета. Положение о государственных трудовых сберегательных кассах Союза Советских Социалистических Республик. 27 ноября 1925 г. // Известия ЦИК Союза ССР и ВЦИК. 1925. № 278.

78. Постановление ЦИК и СНК. Положение о кооперативном кредите. 18 января 1927 г. // Известия ЦИК Союза ССР и ВЦИК. 1927. № 20.

79. Постановление Центрального Исполнительного Комитета и Совета Народных Комиссаров СССР. О принципах построения кредитной системы. 1927 г. // Собрание законов СССР. 1927. № 35. Ст. 364.

80. Постановление Совета Министров СССР. Об утверждении Устава Государственных трудовых сберегательных касс СССР. 11 июля 1977 г. // Решения партии и правительства по хозяйственным вопросам: Сборник документов. Т. 12. Июль 1977 г. март 1979 г. М.: Политиздат, 1979.

Монографии и иные книги

81. Индикаторы цифровой экономики: 2022: статистический сборник / Г.И. Абдрахманова., С.А. Васильковский, К.О. Вишневский, Л.М. Гохберг и др., И60 Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2023. 332 с.

82. Акопов Г.Л. Информационное право: учебное пособие. Ростов н/Д: Феникс, 2008. 348 с.

83. Андреева Г.Н., Бадальянц С.В., Богатырева Т.Г. [и др.] Развитие цифровой экономики в России как ключевой фактор экономического роста и повышения качества жизни населения: монография. Н. Новгород: Проф. наука, 2018. 131 с.

84. Арефа Н.И. Устав Государственного Банка. СПб., 1895. 306 с.

85. Бачило И.Л. Информационное право: учебник. М.: Юрайт, 2011. 512 с.

86. Боер В.М., Павельева О.Г. Информационное право: учеб. пособие. Ч. 1 / ГАУП. СПб., 2006. 116 с.

87. Вайпан В.А. Право и цифровая экономика // Современные информационные технологии и право: монография / А.С. Ворожевич [и др.]; отв. ред. Е.Б. Лаутс; Моск. гос. ун-т им. М.В. Ломоносова, Юрид. ф-т. М.: Статут, 2019. 288 с.

88. Василевская Л.Ю., Подузова Е.Б., Тасалов Ф.А. Цифровизация гражданского оборота: big data в механизме гражданско-правового регулирования (цивилистическое исследование): монография: в 5 т. Т. 5 / отв. ред. Л.Ю. Василевская. М.: Проспект, 2023. 304 с.

89. Ворожевич А.С. Исключительные права в цифровой сфере: объекты, границы, пределы осуществления (комментарий законодательства) // Современные информационные технологии и право: моногр. / отв. ред. Е.Б. Лаутс. М.: Статут, 2019. С. 208-233.

90. Воройский Ф.С. Информатика. Новый систематизированный толковый словарь-справочник. М.: ФИЗМАТЛИТ, 2003. 760 с.

91. Гаврилов Э.П. Советское авторское право: основные положения, тенденции развития. М.: Наука, 1984. 222 с.

92. Гайдаенко Ш.Н., Грачев Д.О., Лещенков Ф.А. и др. Договоры в гражданском праве зарубежных стран: монография / отв. ред. С.В. Соловьева. М.: НОРМА, 2018. 336 с.

93. Городов О.А. Интеллектуальная собственность: правовые аспекты коммерческого использования. СПб., 1999. 32 с.

94. Городов О.А. Информационное право: учебник для бакалавров. М.: Проспект, 2015. 304 с.

95. Заславская Н.М. Информационное обеспечение в цифровом обществе (на примере государственного экологического управления) // Цифровые

технологии и право: сб. науч. тр. I Междунар. науч.-практ. конф. / под ред. И.Р. Бегишева [и др.]. Казань: Познание, 2022. Т. 1. 358 с.

96. Зенин И.А. Основы гражданского права России (конспект лекций для специалистов по праву интеллектуальной собственности). М., 1993. 288 с.

97. Информационное право: учебник для бакалавриата, специалитета и магистратуры / под ред. М.А. Федотова. М.: Юрайт, 2019. 497 с.

98. Карапетов А.Г. Договорное и обязательственное право (общая часть): постатейный комментарий к ст. 307-453 ГК РФ / А.Г. Карапетов [и др.]. М.: Статут, 2017. 1118 с.

99. Керимов Д.А. Законодательная деятельность советского государства. М.: Госюриздат, 1995. 240 с.

100. Кирсанова Е.Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: монография. М.: Юстицинформ, 2022. 288 с.

101. Ковалева Н.Н. Информационное право России: учебное пособие. М.: Дашков и К, 2007. 360 с.

102. Копылов В.А. Информационное право: учебник. 2-е изд., перераб. и доп. М.: Юристъ, 2004. 512 с.

103. Кучеров И.И. Налоговая тайна: правовой режим защиты информации / И.И. Кучеров, А.В. Торшин. М.: ЮрИнфоР, 2003. 329 с.

104. Латино-русский словарь: 16 000 слов / сост. Д.И. Фомицкий; авт. соврем. ред. Л.Ф. Цымлова, Т.А. Ширяева. Ростов н/Д: Феникс, 2001. 701 с.

105. Лысак И.В. Формирование персональной идентичности в условиях сетевой культуры: монография / И.В. Лысак, Л.Ф. Косенчук. М.: Спутник+, 2016. 147 с.

106. Налоговое право. Общая часть: в 2 т. Т. 2: учебник и практикум для академ. бакалавриата / под ред. И.И. Кучерова. М.: Юрайт, 2016. 543 с.

107. Наумов В.Б. Вопросы развития терминологии в сфере персональных данных // Понятийный аппарат информационного права: сборник научных работ / под ред. И.Л. Бачило, Э.В. Талапиной. М., 2015. 278 с.

108. Попондопуло В.Ф. Коммерческое (предпринимательское) право: учебник. М.: Юристъ, 2005. 668 с.

109. Рассолов И.М. Информационное право: учебник для магистров. М.: Юрайт, 2015. 444 с.

110. Розенберг В.В. Промысловая тайна. СПб.: М-во фин., 1910. 68 с.

111. Российское законодательство X-XX веков. В 9 т. Т. 9. / под общ. ред. чл - кор. АЕН РФ, д.ю.н., проф. О.И. Чистякова. М., 1994. 351 с.

112. Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (постатейный). М.: Статут, 2015. 320 с.

113. Санникова Л.В., Харитонова Ю.С. Цифровые активы: правовой анализ: монография. М.: 4 Принт, 2020. 304 с.

114. Сергеев А.П. Гражданское право: учебник / под ред. А.П. Сергеева, Ю.К. Толстого. М., 1998. Ч. 3. 591 с.

115. Тихомиров Ю.А. Курс административного права и процесса. М.: Юринформцентр, 1998. 798 с.

116. Трутнев Д.Р. Архитектура информационных систем. Основы проектирования: учебное пособие. СПб.: НИУ ИТМО, 2012. 66 с.

117. Храмов А.Д. Индустрия 4.0 и Качество 4.0: Особенности влияния на современную промышленность // Основные тенденции развития инновационного предпринимательства в реальном секторе экономики в эпоху цифровизации: вызовы и возможности. М.: ИП Сафронов Р.А., 2021. 299 с.

118. Цифровая экономика: актуальные направления правового регулирования / М.О. Дьяконова, А.А. Ефремов, О.А. Зайцев [и др.]; под ред. И.И. Кучерова, С.А. Синицына. М.: ИЗиСП, НОРМА, 2022. 376 с.

119. Блажеев В. В. Цифровое право: учебник / В.В. Блажеев, М.А. Егорова. - Москва: Проспект, 2020. 637 с.

120. Шершеневич Г.Ф. Учебник торгового прав. М.: СПАРК, 1994. 335 с.

Диссертации и авторефераты

121. Амирбеков К.И. Правообеспечительная юридическая деятельность: проблемы теории и практики : дис. … д-ра юрид. наук: 12.00.01. Сев.-Кавказ. акад. гос. службы. Ростов н/Д, 2006. 46 с.

122. Ашихмин И.М. Международно-правовое обеспечение экологической безопасности в военной деятельности : дис. … канд. юрид. наук: 12.00.10. М., 1997. 199 с.

123. Белых В.С. Гражданско-правовое обеспечение качества продукции, работ, услуг : автореф. дис. … д-ра юрид. наук: 12.00.03. Екатеринбург, 1994. 54 с.

124. Беляев М.В. Объекты и субъекты права на коммерческую тайну: автореф. дис. … канд. юрид. наук: 12.00.14. М., 2005. 26 с.

125. Бондарь И.В. Тайна по российскому законодательству (проблемы теории и практики): дис. … канд. юрид. наук: 12.00.01. Нижний Новгород, 2004. 203 с.

126. Ворникова Е.Д. Правовое регулирование внешней торговли услугами в цифровой экономике: дис. … канд. юрид. наук: 5.1.3. М., 2023. 236 с.

127. Даниленко С.А. Правовое регулирование банковской тайны: автореф. дис. … канд. юрид. наук: 12.00.03. М., 2007. 24 с.

128. Жернова В.М. Правовой режим информационных систем: дис. … канд. юрид. наук: 12.00.13. Челябинск, 2017. 213 с.

129. Зайченко Е.В. Информационное обеспечение в гражданском и арбитражном процессе: дис. … канд. юрид. наук: 12.00.15. Моск. гос. университет. М., 2013. 290 с.

130. Зверева Е.А. Правовое регулирование информационного обеспечения предпринимательской деятельности в Российской Федерации: дис. … д-ра юрид. наук: 12.00.03. Моск. гос. юр. акад. М., 2007. 422 с.

131. Зенцова С.А. Источник повышенной опасности и его уголовно-правовое значение: автореф. дис. ... канд. юрид. наук: 12.00.08. Науч.-исслед. ин-т Федерал. службы исполнения наказаний. М., 2006. 25 с.

132. Карцхия А.А. Гражданско-правовая модель регулирования цифровых технологий: дис. … д-ра юрид. наук: 12.00.03. М., 2019. 445 с.

133. Кирсанова Е.Е. Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике: дис. … канд. юрид. наук: 12.00.03. М., 2021. 188 с.

134. Костенко М.Ю. Правовые проблемы налоговой тайны: дис. … канд. юрид. наук: 12.00.14. М., 2002. 146 с.

135. Красинский В.В. Правовое обеспечение защиты конституционного строя России в избирательном процессе: автореф. дис. … д-ра юрид. наук: 12.00.02. М., 2011. 48 с.

136. Кулешов Г.Н. Административно-правовое регулирование информационного обеспечения в системе государственной гражданской службы Российской Федерации: дис. … канд. юрид. наук: 12.00.14. Моск. гум. университет. М., 2010. 223 с.

137. Куликова Е.В. Влияние новых технологий на развитие авторского права и смежных прав: договоры, законодательство, практика: автореф. дис. … канд. юрид. наук: 12.00.03. М., 2001. 31 с.

138. Лаутс Е.Б. Правовое обеспечение стабильности рынка банковских услуг: автореф. дис. … канд. юрид. наук: 12.00.03. М., 2007. 34 с.

139. Лопатин В.Н. Информационная безопасность России: дис. … д-ра юрид. наук: 12.00.01. СПб., 2000. 433 с.

140. Маркелова К.А. Банковская тайна: правовые аспекты: дис. … канд. юрид. наук: 12.00.12. Саратов, 2000. 184 с.

141. Минбалеев А.М. Система информации: теоретико-правовой анализ: дис. … канд. юрид. наук: 12.00.14. Челябинск, 2006. 272 с.

142. Мытарев Ф.Ю. Правовое регулирование информационного обеспечения субъектов малого и среднего предпринимательства: автореф. дис. … канд. юрид. наук: 12.00.14. М., 2007. 26 с.

143. Насонова Е.Н. Информация как объект гражданского права: дис. … канд. юрид. наук: 12.00.03. М., 2002. 185 с.

144. Редкоус В.М. Административно-правовое обеспечение национальной безопасности в государствах участниках СНГ: автореф. дис. … д-ра юрид. наук: 12.00.14. М., 2011. 48 с.

145. Стахов А.И. Административно-публичное обеспечение безопасности в РФ : автореф. дис. … д-ра юрид. наук: 12.00.14. М., 2007. 35 с.

146. Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. … д-ра юрид. наук: 05.13.19. М., 2004. 52 с.

147. Токолов А.В. Правовое регулирование информационных отношений в сфере цифровых финансовых активов: дис. … канд. юрид. наук: 12.00.13. М., 2022. 215 с.

148. Уварова А.В. Правовое регулирование сделок взаимного кредитования в Российской Федерации и зарубежных странах: дис. … канд. юрид. наук: 12.00.03. М., 2021. 172 с.

149. Шевердяев С.Н. Проблемы конституционно-правового регулирования информационных отношений в Российской Федерации: дис. … канд. юрид. наук: 12.00.02. М., 2002. 210 с.

Статьи

150. Авакьян С.А. Задачи конституционного права в аспекте защиты (от) информации // Конституционное и муниципальное право. 2022. № 8. С. 3-11.

151. Азархин А.В., Карев Д.А., Михайлова М.С. Понятие и классификация правовых принципов // Евразийская адвокатура. 2020. № 1 (44). С. 99-103.

152. Алексеенко А.П. Регулирование деятельности электронных платформ по Закону КНР «Об электронной коммерции» // Юрист. 2020. № 7. С. 62-68.

153. Алешкова И.А., Власова Т.В. К вопросу о принципах права // Вестник Кыргызско-Российского славянского университета. 2019. Т. 19. № 7. С. 79-83.

154. Алимов Э.В., Малютин Н.С. Правовые позиции Конституционного Суда Российской Федерации по вопросам генетической истории семьи и суррогатного материнства // Журнал Белорусского государственного университета. Право. 2020. № 3. С. 1-8.

155. Амирбеков К.И. Правообеспечительная юридическая деятельность // Государство и право. 2006. № 1. С. 88-94.

156. Амиржан К.Ж. Информационные правоотношения: общетеоретический аспект // Вестник Омского университета. Серия: Право. 2017. № 1 (50). С. 31-35.

157. Анцупов Д.В. Актуальные изменения и проблемы коммерческой тайны // Образование и право. 2016. № 1. С. 197-200.

158. Архипов В.В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9. С. 69-90.

159. Архипов В.В. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности / В.В. Архипов, В.Б. Наумов // Закон. 2017. № 5. С. 157-170.

160. Беликов Е.Г. Развитие финансово-правовых принципов в условиях цифровой экономики // Вестник Университета имени О.Е. Кутафина. М.: МГЮА, 2020. С. 39-45.

161. Белоусов А.Л. Теоретические и практические аспекты формирования финансового маркетплейса в Российской Федерации // Russian Journal of Economics and Law. 2021. Т. 15. № 3. С. 413-424.

162. Березина Е.А. Использование смарт-контракта как правовая технология: отечественная и зарубежная законодательная практика // Правовое государство: теория и практика. 2021. № 1 (63). С. 97-118.

163. Богданова Е.Е. Проблемы применения смарт-контрактов в сделках с виртуальным имуществом // Lex russica. 2019. № 7. С. 108-118.

164. Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5-18.

165. Вайпан В.А. Цифровое право: истоки, понятие и место в правовой системе// Право и экономика. 2024. № 1. С. 5-27.

166. Валеева Г. В. Цифровой след и цифровая тень в контексте цифрового образования // Гуманитарные ведомости ТГПУ им. Л. Н. Толстого. 2023. № 4 (48). С. 59-67.

167. Варламова А.Н. Цифровизация как механизм развития конкуренции на отраслевых товарных рынках (на примере рынка электроэнергии) // Бизнес, менеджмент и право. 2023. № 2. С. 38-44.

168. Витко В. Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта // Интеллектуальная собственность. Авторское право и смежные права. 2019. № 2. С. 5-22.

169. Войниканис Е.А., Семенова Е.В., Тюляев Г.С. Искусственный интеллект и право: вызовы и возможности самообучающихся алгоритмов // Вестник Воронежского государственного университета. Серия: Право. 2018. № 4. С. 137-148.

170. Волос А.А. Система принципов-методов гражданского права: постановка проблемы // Ленинградский юридический журнал. 2016. № 3. С. 97-98.

171. Волос А.А. Смарт-контракты и принципы гражданского права // Российская юстиция. 2018. № 12. С. 5-7.

172. Волчинская Е.К. Коммерческая тайна в системе конфиденциальной информации // Информационное право. 2005. № 3. С. 17-21.

173. Гаврин Д.А. Особенности совершения сделок с использованием финансовой платформы // Российское право: образование, практика, наука. 2021. № 5. С. 29-35.

174. Гасанова А.Н. Принципы права: современные подходы // Правовое регулирование в современной России. 2014. № 5 (44). С. 41-45.

175. Гузнов А., Михеева Л., Новоселова Л. и др. Цифровые активы в системе объектов гражданских прав // Закон. 2018. № 5. С. 16-30.

176. Гурко А. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 12. С. 7-18.

177. Демичев А.А. Позитивистская классификация принципов гражданского процессуального права Российской Федерации // Арбитражный и гражданский процесс. 2005. № 7. С. 7.

178. Джан Л., Чен С. Цифровая экономика Китая: возможности и риски // Вестник международных организаций: образование, наука, новая экономика. 2019. Т. 14. № 2. С. 275-303.

179. Дмитриев С.Д. К вопросу о понятии принципов права // Пробелы в российском законодательстве. 2009. № 4. С. 62-64.

180. Дрожжинов В.И., Куприяновский В.П., Евтушенко С.Н., Намиот Д.Е. Стратегический подход к формированию цифрового правительства США // International Journal of Open Information Technologies. 2017. № 4. С. 29-54.

181. Егорова М.А., Ефимова Л.Г. Понятие и особенности правового регулирования криптовалют // Предпринимательское право. 2019. № 3. С. 14-16.

182. Жернова В.М. Информационные системы как источник повышенной опасности в условиях цифровизации // Вестник ЮУрГУ. Серия «Право». 2019. № 3. С. 67-71.

183. Исмаилов И.Ш. Правовое регулирование финансовых платформ и маркетплейсов в контексте развития инструментов финансирования бизнеса: отечественный и зарубежный опыт // Финансовое право. 2022. № 11. С. 26-32.

184. Ишеков К.А., Бокова Л.Н. Правовое регулирование использования информационных технологий в сфере образования // Конституционное и муниципальное право. № 1. 2025. С. 45-48.

185. Карелина С.А., Фролов И.В. Правовой режим криптовалюты и институт несостоятельности (банкротства): проблемы правовой регламентации // Право и цифровая экономика. 2019. № 4(6). С. 14-18.

186. Карцхия А.А. Цифровые технологические (онлайн) платформы: российский и зарубежный опыт регулирования // Гражданское право. 2019. № 3. С. 25-28.

187. Кашкин, С. Ю., Алтухов, А. В., Пожилова, Н. А. Платформенное право как инструмент инновационных инвестиционных платформ (краудфандинг) // Вестник Университета имени О. Е. Кутафина. 2021. № 1 (77). С. 157-166.

188. Климшен И. И., Нигамадзянов А.Р., Гурьянов К.А., Овод И.В. Принцип равенства участников гражданских правоотношений // Colloquium-journal. 2021. № 2. С. 35-38.

189. Ковалева Н.Н. Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций (научный обзор) / Н.Н. Ковалева, Н.А. Жирнова // Информационное право. 2024. № 1 (79). С. 40-43.

190. Ковалева Н.Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта / Н.Н. Ковалева, Н.А. Жирнова // Журнал российского права. 2024. Т. 28, № 7. С. 109-121.

191. Ковлакас Н.В. Нравственные основы правоприменительной практики // Вестник Таганрогского института им. А.П. Чехова. 2009. Специальный выпуск. С. 56-60.

192. Кокорин И. С., Игбаев З. Р. Развитие коммерческой тайны в России (историко-правовой аспект) // Ленинградский юридический журнал. 2011. № 1. С. 94-99. URL: https://cyberleninka.ru/article/n/razvitie-kommercheskoy-tayny-v-rossii-istoriko-pravovoy-aspekt (дата обращения: 14.02.2021).

193. Колюшин Е.И. Инновационные технологии избирательного процесса в свете верховенства закона // Правосудие. 2021. № 3 (3). С. 124-150.

194. Короткина А.С. Информационные системы как объект права // Закон и право. 2022. № 5. С. 43-50.

195. Косенчук Л.Ф. Сущность идентичности и основные подходы к ее исследованию // Теория и практика общественного развития. 2014. № 16. С. 223-225.

196. Крохина Ю.А. Правовой режим защиты налоговой информации и вопросы его оптимизации // Налоги и финансы. 2015. № 3 (27). С. 40-45.

197. Куваева Ю.В., Чудиновских М.В. Мировая практика трансформации подходов к регулированию краудфандингов // Вестник НГУЭУ. 2020. № 3. С. 114-128.

198. Кузнецов П.У., Харитонова Ю.С. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 1. С. 154-161.

199. Кусова Е.А. Информационно-правовое обеспечение государственного управления // Вестник ТГУ. 2011. № 4. С. 292-295.

200. Кучеров И.И., Торшин А.В. Налоговозначимая информация в составе охраняемой экономической информации // Финансовое право. 2001. № 1. С. 25.

201. Лебедева Е.А., Сладкова А.В. О цифровых технологиях контроля в государственном управлении в зарубежных странах // Административное право и процесс. 2020. № 7. С. 83-88.

202. Левчук С.В. Актуальные проблемы использования смарт-контрактов в предпринимательской деятельности // Экономика. Право. Общество. 2022. Т. 7. № 1 (29). С. 16-22.

203. Лисаченко А.В. Правовой режим «больших геномных данных»: за и против свободного обращения // Российский юридический журнал. 2022. № 2. С. 140-151.

204. Лукашевич С.А. Некоторые аспекты гражданско-правового статуса информации // Вопросы российского и международного права. 2021. Т. 11. № 2А. С. 33-39.

205. Малюк А.А., Морозов А.В. Формирование цифровой экономики и проблемы совершенствования нормативно-правового регулирования в области обеспечения информационной безопасности // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 21-36.

206. Медведев Д.А. Новая реальность: Россия и глобальные вызовы // Вопросы экономики. 2015. № 10. С. 5-29.

207. Минбалеев А.В. Правовая природа больших данных // Вестник ЮУрГУ. Серия «Право». 2024. Т. 24, № 3. С. 88-93.

208. Михеева И.Е. Отдельные правовые особенности залога цифровых прав // Право и экономика. 2022. № 10. С. 18.

209. Михеева Л.Ю. Объекты гражданских прав: правовые позиции, содержащиеся в Постановлении Пленума Верховного Суда Российской Федерации «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» // Судья. 2015. № 10. С. 11-18.

210. Морхат П.М. Концепт «электронного лица» в классификации субъектного состава лиц в гражданском праве // Пермский юридический альманах. 2019. № 2. С. 273-282.

211. Морозов А.В. Регулирование рынка криптовалют (информационно-правовой аспект) // Вестник Московского университета. Серия 26. Государственный аудит. 2019. № 2. С. 6-12.

212. Мосин С.А. Свойства конституционных принципов // Правоприменение. 2021. № 3. С. 126-136.

213. Мутасова М.А. Проблема законодательного закрепления принципа справедливости // Социально-экономические явления и процессы. 2015. Т. 10. № 7. С. 172-183.

214. Никитин А.В. О правовом режиме бумажных документов // Российский юридический журнал. 2015. № 4. С. 75-80.

215. Новоселова Л. «Токенизация» объектов гражданского права // Хозяйство и право. 2017. № 12. С. 29-44.

216. Новоселова Л., Габов А., Савельев А. и др. Цифровые права как новый объект гражданского права // Закон. 2019. № 5. С. 31-54.

217. Овчинн Овчинников А.И., Фатхи В.И. Цифровые права как объекты гражданских прав // Философия права. 2019. № 3 (90). С.104-112.

218. Панарина М.М. Наследование аккаунта в социальных сетях и вопросы цифрового наследования: правовое исследование // Наследственное право. 2018. № 3. С. 29-30.

219. Панченко В.Ю., Власенко В.Н. Принципы и нормы права как абстрактные и конкретные правовые регуляторы // Российское правосудие. 2020. № 1. 14-20.

220. Поляков Д.Н. Комбинированные механизмы правовой охраны программного обеспечения в трансграничной предпринимательской деятельности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2021. № 3. С. 243-250.

221. Поляков М.П. Принцип как мировоззренческая идея относительно сущего и должного: новый подход к постижению концептуальной сущности понятия принципов отечественного уголовного процесса // Юридическая техника. 2020. № 14. С. 493-496.

222. Попондопуло В.Ф. Правовые формы цифровых отношений // Юрист. 2019. № 6. С. 29-36.

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

224. Ролинсон П., Ариевич Е.А., Ермолина Д.Е. Объекты интеллектуальной собственности, создаваемые с помощью искусственного интеллекта: особенности правового режима в России и за рубежом // Закон. 2018. № 5. С. 63-71.

225. Рожкова М.А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым [Электронный ресурс] // Закон.ру. 2018. 13 июня. URL: https://zakon.ru/blog/2018/06/13/cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym (дата обращения: 26.10.2024).

226. Рустамов П.А. Договор по оказанию информационных услуг: понятие и свойства // Евразийская адвокатура. 2020. № 2 (45). С. 107-109.

227. Рустамов П.А. Перспективы правового регулирования цифровых валют в Российской Федерации // International Law Journal. 2022. № 7. С. 143-146.

228. Рустамов П.А. К вопросу о совершенствовании правового регулирования краудфандинга в России // Проблемы экономики и юридической практики. 2023. № 1. С. 103-107.

229. Рустамов П.А. К вопросу о совершенствовании правового регулирования цифровых финансовых активов в России // Евразийская адвокатура. 2024. № 1 (66). С. 143-147.

230. Рустамов П.А. Принципы информационно-правового обеспечения цифровой экономики // Евразийская адвокатур. 2024. № 5 (70). С. 189-194.

231. Рустамов П.А. Объекты информационно-правового обеспечения цифровой экономики // Евразийская адвокатура. 2024. №. 6 (71). С. 165-169.

232. Рустамов П.А. О категории информационно-правового обеспечения цифровой экономики // Евразийская адвокатура. 2025. № 1 (72). С. 157-161.

233. Рустамов П.А. Принцип правовой интероперабельности как связующий элемент формирования нормативного ландшафта экономики в условиях цифровизации // Евразийская адвокатура. 2025. № 2 (73). С. 165-170.

234. Рустамов П.А. Совершенствование правового регулирования использования цифрового профиля // Юридический мир. 2025. № 6 (342). С. 41-44.

235. Савельев А.И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32-60.

236. Савельев А.И. Направления регулирования больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5. С. 122-144.

237. Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94-117.

238. Савельев А.И. Некоторые риски токенизации и блокчейнизации гражданско-правовых отношений // Закон. 2018. № 2. С. 36-51.

239. Савельев А.И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127-150.

240. Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43-66.

241. Саменкова С.Е. К вопросу о нормативном закреплении принципов права // Вектор науки Тольяттинского государственного университета. 2012. № 1 (19). С. 204-206.

242. Санникова Л.В., Харитонова Ю.С. Проблемы формирования правовых режимов новых цифровых объектов оборота // Предпринимательское право. Приложение «Право и бизнес». 2019. № 1. С. 37-39.

243. Сафронов В.В. Субъекты информационных правоотношений // Решетневские чтения. 2010. С. 556-557.

244. Северин В.А. Правовое регулирование коммерчески ценной информации // Законодательство. 2000. № 9. С. 36-40.

245. Сергеев А.П., Терещенко Т.А. Большие данные: в поисках места в системе гражданского права // Закон. 2018. № 11. С. 106-123.

246. Синельникова В.Н., Ревинский О.В. Права на результаты искусственного интеллекта // Копирайт. 2017. № 4. С. 17-27.

247. Смирнов Е.Н. Эволюция инновационного развития и предпосылки цифровизации и цифровых трансформаций мировой экономики // Вопросы инновационной экономики. 2018. Т. 8. № 4. С. 553-564.

248. Степаненко Р.Ф., Юн Л.В. Этические основы правоприменительной деятельности: актуальные вопросы теоретического правоведения // Вестник Казанского юридического института МВД России. 2018. № 2 (32). С. 189-196.

249. Суханов Е.А. О гражданско-правовой природе «цифрового имущества» // Вестник гражданского права. 2021. № 6. С. 7-29.

250. Терехова Е.В. Трансграничная передача информации, составляющей коммерческую тайну: проблема правовой квалификации // Актуальные проблемы российского права. 2014. № 3. С. 507-512.

251. Терещенко Л.К. Модернизация информационных процессов и информационного законодательства. [Электронный ресурс]. Режим доступа: СПС «Консультант Плюс».

252. Троян Н.А. Информационно-правовое обеспечение развития национальной системы правовой информации в Российской Федерации в условиях цифровой трансформации // Мониторинг правоприменения. 2020. № 4 (37). С. 28-32.

253. Фатьянов А.А. Тайна как социальное и правовое явление. Ее виды // Государство и право. 1998. № 6. С. 19-28.

254. Хасаншин И.И. Цифровая экономика: понятие и термины // Московский экономический журнал. 2021. № 4. С. 265-274.

255. Цыбулевская О.И., Милушева Т.В. Справедливость в праве: аксиологический подход // Вестник Поволжского института управления. 2017. Т. 17. № 5. С. 52-59.

256. Чаннов С.Е. Правовые угрозы при использовании информационных систем в государственном управлении // Административное право и процесс. 2018. № 9. С. 50-51.

257. Чубукова С.Г. Квазисубъекты в киберправе // Вестник Университета имени О.Е. Кутафина. 2023. № 2 (102). С. 53-61.

258. Чубукова С.Г. Цифровая трансформация системы субъектов информационного права // Вестник Университета им. О.Е. Кутафина (МГЮА). 2019. № 12. С. 74-81.

259. Чурилов А.Ю. Перспективы цифровизации товарораспорядительных документов // Юрист. 2021. № 2. С. 10-11.

260. Шокиров Г.А. Информация как основной объект информационных правоотношений: теоретический и практический аспекты // Вестник Томского государственного университета. 2017. № 415. С. 212-216.

261. Шумилов Ю.П. Моделирование информационных ресурсов // Информационные ресурсы России. 2001. № 6. С. 8-9.

262. Юдина М.А. Индустрия 4.0: перспективы и вызовы для общества // Государственное управление. Электронный вестник. 2017. № 60. С. 197-215.

263. Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. № 2. С. 36-55.

264. Яценко Т.С. Наследование цифровых прав // Наследственное право. 2019. № 2. С. 11-14.

Литература на иностранных языках

265. Abbott R.I Think, Therefore I Invent: Creative Computers and the Future of Patent Law // Boston College Law Review. 2016. Vol. 57. P. 1112-1114.

266. Abelson H. and Lessig L.: ‘Digital identity in Cyberspace’, White paper submitted for 6.805 / Law of Cyberspace: Social Protocols (Dec 1998).

267. Barthes R. Elements of Semiology / Transl. by A. Lavers, C. Smith. N.Y.: Hill and Wang, 1982. 128 p.

268. Burleson W., Carrara S. (eds.) Security and Privacy for Implantable Medical Devices. Berlin: Springer, 2014. 205 p.

269. Computer Care v. Service Sys. Enters., Inc., 982 F.2d 1063, 1074 (7th Cir. 1992) (full text).

270. Changhee K. Legal Studies of Private Enforcement Accompanied by Smart Contracts. The Institute of Legal Studies Inha University, Inha Law review, 2019, vol. 22, no. 1, pp. 465-494. Available at: http://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE07995518#none (дата обращения: 02.03.2025).

271. Eco U. Semiotics and the Philosophy of Language. Bloomington: Indiana University Press, 1986. 256 p.

272. Erlank W. Introduction to Virtual Property: Lex Virtualis IPSA Loquitur // Potchefstroom Electronic Law Journal. 2015. Vol. 18. № 7. [Электронный ресурс]. URL: https://ssrn.com/abstract=2753716.

273. FINMA (16 February 2018). Guidelines for enquiries the regulatory framework for initial coin offerings (ICOs). 16 February 2018. URL: https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

274. Hudkins Ronald E. Your Digital Footprint: Password Protection Requirements. Paperback. June 12, 2014. URL: https://www.scribd.com/book/230559848/Your-Digital-Footprint-Password-Protection-Require-ments.

275. Mesenburg T.L. Measuring the Digital Economy / T.L. Meysenbourg. - U.S. Bureau of the Census, 2001. URL: https://www.census.gov/content/dam/Census/library/working-papers/2001/econ/umdigital.pdf (дата обращения: 03.08.2025).

276. Negroponte N. Being Digital. N.Y.: Knopf, 1995. 243 p.

277. Schemkes F. et al. Blockchain en het recht: Een verkenning van de reguleringsbehoefte. Tilburg, 2019.

278. SEC. Report of Investigation under 21 (a) of the Securities Exchange Act of 1934: The DAO, Release № 81207, and Investor Bulletin: Initial Coin Offerings. 25 July 2017.

279. Shannon C.E., Weaver W. The Mathematical Theory of Communication. Urbana: University of Illinois Press, 1949. 125 p.

280. Skitlon M. Building the Digital Economy Enterprice: A Guide to Constructing Monetization Models Using Digital Technologies. Berlin: Springer. 2015. – Access mode: free. URL: https://books.google.ru/books?id=mtRgCgAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false (дата обращения: 03.08.2025).

281. Solaiman S.M. Legal personality of robots, corporations, idols and chimpanzees: a quest for legitimacy // Artificial Intelligence and Law. 2017. Vol. 25. № 2. P. 155-179.

282. Tapscott D. The Digital Economy: Promise and Peril In The Age of Networked Intelligence. N.Y.: McGrawHill, 1996. 342 p.

283. Wietzenboeck E.M. Electronic Agent and the Formation of Contracts // International Journal of Law and Information Technology. 2001. Vol. 9. № 3. P. 204-234.

Иные источники

284. Berg, T., Burg, V., Gombović, A., Puri, M. On The Rise of FinTechs – Credit Scoring Using Digital Footprints (July 15, 2019). URL: https://www.fdic.gov/analysis/cfr/working-papers/2018/cfr-wp2018-04.pdf. (дата обращения: 02.03.2025).

285. Big Data. URL: https://www.gartner.com/en/informationtechnology/glossary/big-data. [Электронный ресурс]. (дата обращения: 27.07.2023).

286. Digital Economy Definition: 3 Digital Economy Examples. URL: https://www.masterclass.com/articles/digital-economy (дата обращения: 02.03.2025).

287. Digital Government. Building a 21st Century Platform to Better Serve the American People. [Электронный ресурс]: [сайт]. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html (дата обращения: 02.03.2025).

288. Etimad – платформа финансовых цифровых услуг (пер. с араб.). URL: https://portal.etimad.sa/. (дата обращения: 02.03.2025).

289. European Commission. Expert Group on Taxation of the Digital Economy. European Commission, Brussels [Электронный ресурс]. URL: http://ec.europa.eu/taxationcustoms/sites/taxation/files/resources/documents/taxation/gen info /good governance matters/digital/general issues.pdf. (дата обращения: 10.11.2023).

290. How Can You Protect Your Software As A Trade Secret? URL: https://www.khlawfirm.com/how-can-you-protect-your-software-as-a-trade-secret/ (дата обращения: 06.10.2024).

291. Inter-organisational e-government: From four levels of interoperability to seen dimensions of co-gjvernance. 2015. URL: https://www.diva-portal.org/smash/get/diva2:783907/FULLTEXT01.pdf . (дата обращения: 29.07.2025).

292. John Stark. How Close Are Smart Contracts to Impacting Real-World Law? COINDESK (Apr. 11, 2016). URL: http://www.coindesk.com/blockchain-smarts-contractsreal-world-law/. (дата обращения: 02.03.2025).

293. Saudi Arabia market challenges - Official Website of the International Trade Administration. URL: https://www.trade.gov/knowledge-product/saudi-arabia-market-challenges/ (дата обращения: 02.03.2025).

294. What Is the Digital Economy? URL: https://online.wharton.upenn.edu/blog/what-is-the-digital-economy (дата обращения: 02.03.2025).

295. Clack, Christopher D., Bakshi, Vikram A., Braine, Lee. Smart Contract Templates: Foundations, Design Landscape and Research Directions. URL: https://www.researchgate.net/publication/305779577_Smart_Contract_Templates_foundations_design_landscape_and_research_directions_CDClack_VABakshi_and_LBraine_arxiv160800771_2016 (дата обращения: 02.03.2025).

296. Баловсяк Н. Право на убийство: есть ли у людей право уничтожать роботов. URL: https://uip.me/2017/05/people-vs-robots/ (дата обращения: 05.06.2025).

297. Головенчик Г.Г. Цифровая экономика [Электронный ресурс]: учеб.-метод. комплекс. Минск: БГУ, 2020. 1 электрон. опт. диск (CD-ROM).

298. Гришаев С.П., Свит Ю.П., Богачева Т.В. Постатейный комментарий к Гражданскому кодексу РФ [Электронный ресурс] // Режим доступа: СПС «КонсультантПлюс» (дата обращения: 25.07.2025).

299. Декреты Советской власти. Т. 1. М.: Гос. изд-во полит. литературы, 1957. 626 с.

300. Доклад Аналитического центра при Правительстве РФ «Большие данные для государственного управления: опыт внедрения (пилотное

исследование). URL: https://ac.gov.ru/files/content/10087/sorokin-kruglyj-stol-issledovanie-pdf.pdf?ysclid=lsofph8lfv464938404 (дата обращения: 02.03.2025).

301. Единая служба приложений Министерства сельского хозяйства, лесного хозяйства и рыболовной промышленности Японии (eMAFF) (пер. с яп.). URL: https://www.maff.go.jp/j/kanbo/dx/emaff.html (дата обращения: 02.03.2025).

302. Единороги, декакорны и гектакорны: как финтех-индустрия ставит рекорды роста. URL: https://www.forbes.ru/finansy/439263-edinorogi-dekakorny-i-gektakorny-kak-finteh-industria-stavit-rekordy-rosta (дата обращения: 02.03.2025).

303. ИИ Официально получил вид на жительство и ожидает защиты своих прав. [Электронный ресурс]. URL: https://robogeek.ru/iskusstvennyi-intellekt/ii-ofitsialno-poluchil-vid-na-zhitelstvo-i-ozhidaet-zaschity-svoih-prav (дата обращения: 02.03.2025).

304. Исследование по определению состава тайн Итог. — [сайт Сколково]. URL: https://sk.ru/foundation/legal/m/sklegal03/22588/download.aspx. Руководители и соавторы НИР: В.Б. Наумов, В.В. Архипов; исполнители НИР, соавторы: Р.А. Ахобекова, Т.А. Бовсуновская, Я. В. Бутримович, А.В. Грачева, Е.М. Крамм, С.П. Лялькова, В.О. Полыгалов, К.М. Смирнова, Е.В. Тытюк. Объектом исследования выступили законодательство и правоприменительная практика в России, ЕС и входящие в него страны, Великобритании, США, Японии, Сингапуре, Южной Корее, Израиле, ОАЭ и ряде других стран (дата обращения: 02.03.2025).

305. Концепция законодательного регламентирования механизмов организации оборота цифровых валют: электрон. документ. URL: https://rg.ru/2022/02/08/pravitelstvo-utverdilo-koncepciiu-oborota-kriptovaliut-v-rossii.html (дата обращения: 02.03.2025).

306. Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. М.: Фонд развития центра разработки и коммерциализации новых технологий, 2020. 32 с.

307. Классификация криптоактивов: от служебных токенов до платформ // Криптовалюта. URL: https://cryptocurrency.tech/klassifikatsiya-kriptoaktivov-ot-sluzhebnyh-tokenov-do-platform/ (дата обращения: 02.03.2025).

308. Маркетплейсы, краудфандинг и ЦФА: итоги развития платформенных сервисов. URL: https://www.cbr.ru/press/event/?id=14760 (дата обращения 03.08.2023).

309. На ПМЮФ обсудили идентификацию в цифровой среде. URL: https://www.advgazeta.ru/novosti/na-pmyuf-obsudili-identifikatsiyu-v-tsifrovoy-srede/ (дата обращения: 02.03.2025).

310. Национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4. 06. 2019 г. № 7. URL: https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fwww.google.com%2f#section-docs.

311. Национальный проект «Экономика данных и цифровая трансформация государства». URL: https://xn--80aapampemcchfmo7a3c9ehj.xn--p1ai/new-projects/ekonomika-dannykh/.

312. Об итогах социально-экономического развития Российской Федерации в январе — декабре 2021 г. // Официальный сайт Министерства экономического развития Российской Федерации. URL: http://economy.gov.ru/minec/activity/sections/inforientedsoc (дата обращения: 10.11.2023).

313. Обзор платформенных сервисов в России. Операторы инвестиционных платформ, операторы информационных систем и операторы финансовых платформ. Информационно-аналитический материал. М., 2024. URL: https://www.cbr.ru/Collection/Collection/File/49243/platform_services_2024-1.pdf (дата обращения: 02.03.2025).

314. Обзор рынка краудфандинга в России. URL: http://www.cbr.ru/collection/collection/file/42097/crowdfunding_market_01_2022.pdf (дата обращения 03.08.2023).

315. Операторы инвестиционных платформ. URL: https://www.cbr.ru/finm_infrastructure/oper/ (дата обращения 03.08.2023).

316. Отчет по применению риск-ориентированного подхода. Виртуальные активы и провайдеры услуг виртуальных активов. [Электронный ресурс]. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/MUMCFM-FATF-Guidance-RBA-VA-VASPs.pdf.coredownload.inline.pdf (дата обращения: 02.03.2025).

317. Перспективы развития гражданского законодательства в России: планы и современные реалии [Интервью с Е.А. Сухановым] // СПС «КонсультантПлюс» (дата обращения: 20.01.2025).

318. Разработана концепция регулирования краудфандинга в России. URL: https://www.cbr.ru/press/event/?id=712 (дата обращения 03.08.2023).

319. Регулирование big data в России. URL: https://proright.ru/2018/12/03/bigdata/ (дата обращения: 02.03.2025).

320. Россия получила доступ к информации о счетах своих граждан в 80 странах. URL: https://www.nalog.ru/rn78/news/smi/6068722/ (дата обращения: 02.03.2025).

321. Сабо Н. Смарт-контракты. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (дата обращения: 02.03.2025).

322. Сборник приказов Военного Совета республики. 1918. № 97. 990 с.

323. Сухаревская А. Незаметное государство. URL: https://www.vedomosti.ru/partner/articles/2019/12/19/819009-nezametnoe-gosudarstvo (дата обращения: 02.03.2025).

324. Терещенко Т. Что думает законодатель о больших пользовательских данных? URL: https://zakon.ru/blog/2018/10/27/chto_dumaet_zakonodatel_o_bolshih_polzovatelskih_dannyh (дата обращения: 02.03.2025).

325. Торговое уложение Германии. Закон об акционерных обществах. Закон об обществах с ограниченной ответственностью. Закон о производственных и хозяйственных кооперативах. М.: Волтерс Клувер, 2009. 632 с.

326. Тюльканов А. Смарт-контракты – договоры или технологические средства? URL: https://zakon.ru/blog/2017/04/07/smart-kontrakty__dogovory_ili_tehnicheskie_sredstva (дата обращения: 02.03.2025).

327. Устав Автономной некоммерческой организации «Цифровая экономика». URL: https://files.data-economy.ru/Docs/ustav_d-economy.pdf (дата обращения: 02.03.2025).

328. ЦБ и Минэкономразвития собрались по-разному регулировать краудфандинг. URL: https://lenta.ru/news/2018/01/29/crowdfunding (дата обращения: 08.07.2025 г.).

329. ЦБ решил усилить контроль за краудфандингом. URL: https://www.vedomosti.ru/finance/articles/2022/11/22/951451-tsb-reshil-usilit-kontrol-za-kraudfandingom (дата обращения 03.08.2023).

330. «Цифровые активы» выпустили первые токены для участников корпоративной программы «Норникеля» URL: https://nornickel.ru/news-and-media/press-releases-and-news/tsifrovye-aktivy-vypustili-pervye-tokeny-dlya-uchastnikov-korporativnoy-programmy-nornikelya (дата обращения: 02.03.2025).

331. Цифровое будущее: кто будет рулить миром – национальные правительства или транснациональные корпорации. URL: https://www.hse.ru/news/expertise/442058357.html (дата обращения: 22.04.2025).

332. Цифровой двойник. URL: https://digitaltwin.ru/products/digital-twin/ (дата обращения: 02.03.2025).

333. Человекоподобный робот получил гражданство Саудовской Аравии. [Электронный ресурс]. URL: https://www.techinsider.ru/technologies/news-393732-chelovekopodobnyy-robot-poluchil-grazhdanstvo-saudovskoy-aravii/ (дата обращения: 02.03.2025).

334. Эрделевский А.М. О цифровых правах // СПС КонсультантПлюс. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=122169#w4c95nUDLwaxxctW (дата обращения 02.03.2025).

335. ЮАР выдала ИИ-системе первый в мире патент на изобретение. [Электронный ресурс]. URL: https://d-russia.ru/juar-vydala-ii-sisteme-pervyj-v-mire-patent-na-izobretenie.html (дата обращения: 02.03.2025).

336. Японский консорциум по управлению данными (JDMC) принимает решение о вручении наград MAFF за управление данными в 2022 году (пер. с яп.). URL: https://re-how.net/all/1744762/l (дата обращения: 02.03.2025).

Судебная практика

337. Постановление Конституционного Суда РФ от 14 мая 2003 г. № 8-П «По делу о проверке конституционности пункта 2 статьи 14 Федерального закона «О судебных приставах» в связи с запросом Лангепасского городского суда Ханты-Мансийского автономного округа» // Российская газета. 27.05.2003 г. № 99.

338. Определение Конституционного Суда РФ от 28.06.2012 № 1253-О // СПС «КонсультантПлюс».

339. Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 14.01.2020 № 225-АПУ19-4 (текст опубликован не был) // СПС «КонсультантПлюс».

340. Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017 // СПС «КонсультантПлюс».

341. Постановление Тринадцатого арбитражного апелляционного суда от 17.01.2018 № 13АП-30540/2017 по делу № А21-6695/2017 // СПС «КонсультантПлюс».

342. Постановление Арбитражного суда Поволжского округа от 18.05.2023 № Ф06-3649/2023 по делу № А55-7445/2022 // СПС «КонсультантПлюс».

343. Решение Арбитражного суда Приморского края от 24.09.2024 по делу № А51-15065/2024 // СПС «КонсультантПлюс».

344. Решение Арбитражного суда Удмуртской области от 05.11.2024 по делу № А71-18227/2024. URL: https://kad.arbitr.ru/Card/22beb57b-a063-4006-b8a5-4ab83d0acbcc.

345. Решение Дорогомиловского районного суда г. Москвы от 08.02.2021 по делу № 2–304/21. URL: https://mos-gorsud.ru/rs/dorogomilovskij/services/cases/civil/details/03c2ba0f-799c-4920-af7e-84ead7d89958 (дата обращения: 25.07.2025).

346. Решение Таганского районного суда г. Москвы от 01.07.2021 по делу № 2-2418/2021 // СПС «КонсультантПлюс».

347. Решение Савеловского районного суда от 09.11.2021 г. № 2-2888/2021; Апелляционное определение от 28.09.2023 по делу № 33-39520/2023 (в суде 1-й инст. № 2-3411/2023) // СПС «Консультант Плюс».

348. Постановлению мирового судьи судебного участка № 422 по делу об административном правонарушении № 05-3220/422/2021 от 24.12.2021. URL: https://mos-sud.ru/422/cases/admin/details/a600a573-e5a3-4629815c080f3c6220ed?caseDateFrom=&caseDateTo=&caseFinalDateFrom=&caseFinalDateTo=&caseNumber=&codex=&docsDateFrom=&docsDateTo=&documentStatus=&documentType=&hearingRangeDateFrom=&hearingRange (дата обращения: 02.03.2025).

349. Решение Федерального Верховного суда Германии по делу № XII ZR 89/21 URL: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=131670&pos=0&anz=1 (дата обращения: 02.03.2025).