Студенческий научный электронный журнал
StudArctic Forum

ПЕТРОЗАВОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Т. 10, № 4. С. 110–122 **Право** **2025**

Научная статья
УДК 34.096
DOI: 10.24412/2500-140X-2025-4-110-122

КОЖЕВНИКОВ Александр Константинович — магистратура, Уральский институт управления – филиал РАНХиГС при Президенте Российской Федерации (Екатеринбург, Россия), *Alex_kozh00@mail.ru*

ЦИФРОВОЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРАВОВЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Научный руководитель:
Мазеин Артем Владимирович
Рецензент:
Ковригина Екатерина Сергеевна
Статья поступила: 10.10.2025;
Принята к публикации: 15.12.2025;
Размещена в сети: 15.12.2025.

Аннотация. В статье анализируются актуальные проблемы создания Цифрового кодекса РФ как комплексного законодательного акта для регулирования цифровых отношений. Выявляются вызовы современной цифровизации права. Исследуются перспективы формирования единого правового пространства в сфере информационных технологий. Применяются методы сравнительно-правового анализа, системного подхода, элементы правового моделирования, анализ судебной практики и правоприменительного опыта. В результате выявлены ключевые направления развития цифрового законодательства и предложены пути решения существующих правовых коллизий.

Ключевые слова: цифровой кодекс, цифровое право, цифровизация, информационное законодательство, цифровые права, искусственный интеллект, блокчейн, смарт-контракты, правовое регулирование

Для цитирования: Кожевников А. К. Цифровой кодекс Российской Федерации: правовые вызовы и перспективы // StudArctic Forum. 2025. Т. 10, № 4. С. 110–122.

Стремительное развитие цифровых технологий в XXI веке кардинально преобразило характер общественных отношений, сформировав принципиально новую правовую реальность, требующую адекватного нормативного отклика. Сейчас Российская Федерация (далее – РФ) находится перед необходимостью формирования систематизированного правового ответа на многоплановые вызовы цифровой трансформации экономики, государственного управления и социальной жизни.

Актуальность исследования определяется многоуровневой проблематикой. Прежде всего, государству необходимо обеспечить кодификацию и систематизацию законодательства в области информационных технологий. По состоянию на 2024 год в России действует более 60 федеральных законов и несколько сотен подзаконных актов, касающихся информационной сферы, что неизбежно порождает фрагментарность, многозначность норм и противоречивость правового регулирования[1]. Данное обстоятельство препятствует формированию стройной системы юридических гарантий для участников цифровых отношений. При этом цифровая экономика составляет уже 6,5 % валового внутреннего продукта России, и правовая неопределённость становится серьёзным препятствием для её ускоренного развития.

Ключевая проблема состоит в отсутствии единого систематизированного методологического подхода к правовому регулированию цифровых отношений [Даниленко: 84], [Павлова: 4]. Существующее законодательство развивалось реактивно, в ответ на конкретные технологические вызовы и практические потребности, что привело к образованию правовых пробелов, логических противоречий между отдельными нормативными правовыми актами (далее – НПА) и недостаточности механизмов правозащиты. Уникальность и значимость исследования состоит в комплексном анализе концепции Цифрового кодекса как универсального инструмента преодоления фрагментарности цифрового законодательства и последовательного формирования единой правовой парадигмы регулирования цифровых отношений, адекватной вызовам современности.

Целью данного исследования является выявление основных правовых вызовов, теоретических основ и практических перспектив создания Цифрового кодекса РФ как системообразующего акта цифрового права, отвечающего потребностям развития цифровой экономики и защиты прав субъектов цифровых отношений. Для достижения цели необходимо решить следующие задачи:

1) провести комплексный анализ современного состояния правового регулирования цифровых отношений в РФ, выявить и систематизировать основные проблемы, а также определить концептуальные и методологические основы построения Цифрового кодекса, разработать его предполагаемую структуру, определить круг регулируемых отношений и материально-правовых институтов;

2) провести сравнительно-правовой анализ международного опыта разработки и внедрения цифрового законодательства, включая опыт стран-соседей и передовых юрисдикций, а также оценить практические перспективы принятия Цифрового кодекса, выявить потенциальные вызовы и препятствия при его реализации;

3) разработать рекомендации по разрешению имеющихся правовых коллизий и определить направления совершенствования правоприменительной практики в сфере цифровых отношений.

Методология исследования включает применение системно-правового анализа для выявления внутренних связей между различными компонентами цифрового законодательства, а также использование сравнительно-правового метода для изучения опыта других государств. В статье присутствуют элементы правового моделирования при разработке предполагаемой структуры кодекса; анализ судебной практики и прецедентных решений, демонстрирующих необходимость реформирования; метод критического анализа действующих НПА для выявления их недостаточности, а также использование статистического и ситуационного методов при анализе фактических правоприменительных проблем.

* * * * *

Правовое регулирование цифровых технологий в России формировалось на основе многоуровневой системы НПА различной иерархии. Конституционная основа регулирования закреплена в Конституции РФ, где скрыто отражены гарантии защиты информации, права на неприкосновенность частной жизни (ст. 23) и право на доступ к информации (ст. 29). Однако Конституция не содержит специализированных норм, адаптированных к цифровой среде и не предусматривает права на цифровую идентичность.

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149) служит основополагающим базовым актом информационного законодательства. Данный закон был принят в условиях относительной стабильности технологического развития и в своё время

заложил фундамент информационного права РФ. Однако стремительное развитие технологических инноваций потребовало внесения более 60 изменений в указанный закон. Несмотря на множественные корректировки, ФЗ № 149 сохраняет внутреннюю недостаточность: дефиниции остаются абстрактными, механизмы ответственности фрагментарны, а содержание ключевых понятий поддаётся различным толкованиям в судебной практике.

Специализированные законодательные акты, появившиеся позже, включают:

1) Федеральный закон от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации», который регулирует отношения, связанные с доступом граждан, организаций, общественных объединений, органов публичной власти к информации о деятельности судов в РФ;

2) Федеральный закон от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» устанавливает единый порядок доступа граждан и организаций к такой информации;

3) Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» регулирует отношения в области использования электронных подписей;

4) Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», регулирующий обработку персональной информации, однако недостаточно учитывающий специфику больших данных (Big Data) и машинного обучения;

5) Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ № 187), установивший требования к защите критически важных информационных объектов.

Значительным сдвигом в правовом признании цифровых явлений стало внесение изменений в Гражданский кодекс РФ в 2019 году. Федеральным законом от 18 марта 2019 года № 34-ФЗ Гражданский кодекс был дополнен статьей 141.1, впервые закрепившей понятие «цифровые права» как обязательства и иные права, содержание и условия осуществления которых могут быть установлены только в электронной форме и которые не могут быть установлены и осуществляться иным образом. Это стало принципиально важным шагом в признании новых объектов гражданских прав и расширении материально-правовой защиты лиц.

Однако правоприменительная практика незамедлительно выявила недостаточность этого регулирования. По выводам исследователя А.А. Волоса, существующие правила статьи 141.1 Гражданского кодекса создают лишь общие ориентиры и не предусматривают специальных механизмов защиты цифровых прав при их нарушении, хищении или неправомерном использовании [Волос: 16]. Судебная практика показала, что при рассмотрении конфликтов, связанных со взломом аккаунтов, кражей электронных кошельков или незаконным распоряжением цифровыми активами, суды испытывают затруднения в применении существующих норм и часто обращаются к аналогии закона, что снижает предсказуемость судебных решений.

Федеральный закон от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ № 259), представил первое комплексное нормативное регулирование криптовалют и иных цифровых финансовых активов. Данный закон ввёл легальное определение цифровых финансовых активов, установил порядок их учёта и обращения. Однако существенным пробелом этого закона является отсутствие норм, регулирующих смарт-контракты – самоисполняемые цифровые контракты, действующие на основе заранее запрограммированного алгоритма. Федеральный закон № 259 вообще не использует термин «смарт-контракт», что оставляет правовой режим этих инструментов в

состоянии неопределённости и создаёт риск судебных конфликтов при разрешении споров об ответственности за нарушение условий программируемых обязательств.

Новаторским подходом к регулированию цифровых инноваций стало создание специальных экспериментальных правовых режимов. Федеральный закон от 31 июля 2020 года № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» предусмотрел возможность установления специальных правил для тестирования инновационных технологических решений на ограниченных территориях и на определённый срок. К 2024 году данный механизм продемонстрировал значительную эффективность, особенно в сфере апробации систем искусственного интеллекта (далее – ИИ): режим «Москва» позволил провести стартап-проекты с использованием ИИ-систем в различных административных и коммерческих процессах, получив практические данные об их функционировании и выявив необходимые правовые корректировки.

Ключевым направлением защиты цифровой среды стало обеспечение кибербезопасности. Федеральный закон № 187 установил обязательные требования к защите критической информационной инфраструктуры, определил субъектов, обязанных обеспечивать эту защиту, и ввёл систему мониторинга и уведомления об инцидентах. Соответственно, Уголовный кодекс РФ был дополнен статьей 274.1, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру. Однако правоприменительная практика выявила сложности в определении границ применения этой статьи, в разграничении компетенции различных правоохранительных органов и судов при рассмотрении таких дел.

Первой и наиболее фундаментальной проблемой законодательства является отсутствие единого, непротиворечивого понятийного аппарата. Ключевые термины, такие как «информационная система», получают принципиально различную трактовку в зависимости от того, в каком НПА они используются, что неминуемо порождает коллизии при правоприменении [Жернова: 19], [Апт: 66].

Утративший силу Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» определял это понятие косвенно, через перечисление целей и функциональных назначений, что создавало широкое поле для интерпретаций. В действующем ФЗ № 149 информационная система определена как «совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств». Это определение, казалось бы, более конкретно, однако и оно оставляет пространство для манёвра и неоднозначного толкования. В результате судебная практика и правоприменительная деятельность нередко приводят к противоречивым решениям относительно того, является ли тот или иной функциональный комплекс информационной системой в смысле законодательства, имеет ли это отношение к критической инфраструктуре и, следовательно, подлежит ли особому режиму защиты.

Ещё более остро эта проблема проявляется при попытке отнести к тому или иному правовому статусу ведомственные системы, используемые в государственном управлении. Отсутствие ясных критериев приводит к тому, что одна и та же система может классифицироваться по-разному в зависимости от позиции конкретного органа власти или судьи.

Второй системной проблемой является принципиальное отставание темпа развития законодательства от скорости технологических инноваций. Такие явления, как генеративный искусственный интеллект (системы, способные порождать новый контент на основе обучения на больших массивах данных), создают острые вопросы о правах интеллектуальной собственности на создаваемый ими контент, об ответственности за ошибки и галлюцинации нейросетей, однако законодательство остаётся молчаливым в отношении этих проблем.

Не менее важны вопросы, связанные с NFT (non-fungible tokens – невзаимозаменяемые токены), которые оставляют открытыми правовые загадки о статусе и механизмах защиты виртуальной собственности, о применимом праве при их обороте и о способах судебной защиты прав на них.

Явление метавселенных (распределённых цифровых пространств, в которых физические лица и юридические лица могут взаимодействовать через аватары) стирает границы между реальным и цифровым миром, ставя перед правом вопросы о статусе отношений, возникающих в этих пространствах, о юрисдикции и применимом праве [Джендубаева: 107]. Неясно, подлежат ли обычному правовому регулированию контракты, заключённые в метавселенной, или они требуют специального регулирования.

По оценкам экспертов, проникновение высокотехнологичных решений в сферу правоприменения не превышает 15 %[2], что красноречиво свидетельствует о масштабе отставания судебной и правоохранительной систем от требований времени.

Третья системная проблема вытекает из глобальной, трансграничной природы цифровой среды [Ситников: 51], [Полежаев: 199]. Большинство значимых цифровых платформ, сервисов и технологий контролируются международными корпорациями, часто зарегистрированными в юрисдикциях, находящихся за пределами РФ. Это порождает острые вопросы об определении применимого права, о международной юрисдикции и о механизмах признания и исполнения судебных решений.

Яркой и показательной иллюстрацией данного вызова стал конфликт с Google. В 2022–2024 годах российские суды наложили на компанию Google значительные административные штрафы за неповиновение требованиям российского законодательства относительно удаления запрещённого контента[3]. Google оспорил данные штрафы, апеллируя к своему статусу как компании, зарегистрированной в США, и утверждая, что российское законодательство о защите информации выходит за пределы должного применения.

Международный арбитражный суд в Великобритании, рассмотрев спор в 2024 году, постановил, что действия России представляют собой форму «согласованной стратегии международного принуждения» и признал наложенные штрафы несоответствующими нормам международного права. Позже, в январе 2025 года, Высокий суд Англии и Уэльса издал решение, запрещающее российским телеканалам (RT и другим) судиться с Google по вопросу о блокировке их YouTube-каналов, согласившись с позицией, что такие споры должны регулироваться британским законодательством, а не российским. Эти решения наглядно демонстрируют, как национальное право сталкивается с сопротивлением глобальных цифровых платформ, а попытки регулирования превращаются в инструмент политико-правового противостояния, что требует принципиально иного подхода к формированию правовой базы.

Идея создания Цифрового кодекса была впервые предложена в рамках Стратегии развития отрасли связи РФ на период до 2035 года, утверждённой Распоряжением Правительства РФ от 24.11.2023 № 3339-р. Согласно концептуальному видению Министерства цифрового развития, связи и массовых коммуникаций РФ (далее – Минцифры), кодекс должен был стать «комплексным сводом всего законодательного регулирования, которое касается вопросов цифровизации, развития и использования цифровых технологий, защиты данных, цифровых прав и цифровой безопасности»[4]. По первоначальному плану Минцифры, первая версия проекта была запланирована на представление в середине 2025 года, при этом внесение его в Государственную Думу РФ планировалось на конец 2025 года.

Однако реализация этого проекта встретила значительное препятствие. В декабре 2023 года Совет при Президенте РФ по кодификации и совершенствованию гражданского

законодательства рассмотрел концепцию Цифрового кодекса и не поддержал инициативу, указав на серьёзные проблемы нечеткости предмета регулирования, неопределённости с границами применения кодекса и сомнения в целесообразности кодификации в условиях динамичного развития технологий[5]. Несмотря на скептицизм, практическая разработка проекта продолжалась. На основе пояснительных материалов и проектных документов можно реконструировать предполагаемую структуру кодекса.

Общая часть должна содержать:

- базовые принципы цифрового права (технологическая нейтральность, открытость и прозрачность алгоритмов, минимизация вмешательства в приватность, цифровой суверенитет);
- единый понятийный аппарат и систему дефиниций, применимую ко всем сферам цифрового права;
- основания и порядок установления правового статуса субъектов цифровых отношений (разработчиков, операторов, пользователей, администраторов систем);
- общие механизмы защиты прав и ответственности в цифровой среде.

Особенная часть планировалась для регулирования специфических институтов и технологий:

- ИИ (определение правового статуса ИИ-систем, механизмы их сертификации, установление режимов ответственности за решения, принимаемые ИИ-системами, принципы этичного и безопасного использования);
- блокчейн и распределённые реестры (правовой режим криптографических подписей, определение статуса смарт-контрактов как юридически признанных инструментов);
- большие данные (регулирование сбора, обработки, хранения и использования больших объёмов информации, баланс между инновационным использованием данных и защитой приватности);
- интернет вещей (правовой режим устройств, автоматически генерирующих и передающих данные, вопросы их ответственности);
- цифровые товары и услуги (механизмы защиты потребителей в цифровой среде, регулирование цифровых платформ);
- киберпреступность и кибербезопасность (уточнение ответственности за различные формы незаконного воздействия на цифровые инфраструктуры).

Практический прогресс в разработке цифрового законодательства был достигнут в других странах. 18 июня 2025 года Парламент Кыргызской Республики принял Закон о Цифровом кодексе (закон КР от 31 июля 2025 года № 178), который стал первым в пространстве СНГ полнофункциональным кодификационным актом в этой сфере[6]. Кыргызский кодекс включает комплексное регулирование цифровых отношений, определяет статус цифровых прав, устанавливает правила для ИИ и смарт-контрактов.

В Азербайджанской Республике и Республике Казахстан проекты цифровых кодексов находятся в расширенной стадии разработки и уже прошли обсуждение на уровне правительственных органов. В Республике Узбекистан кодекс находится на завершающей стадии подготовки и готов к внедрению в законодательную практику.

На международном уровне наблюдается динамичное развитие подходов к цифровому регулированию. Европейский Союз разработал и принял несколько комплексных актов:

1) AI Act (закон об искусственном интеллекте, вступивший в силу в 2024 году) устанавливает дифференцированный режим регулирования в зависимости от степени риска ИИ-систем;

2) Digital Services Act регулирует деятельность цифровых платформ и устанавливает ответственность за контент;

3) Digital Markets Act адресован доминирующим цифровым платформам и ограничивает их антиконкурентное поведение.

Сингапур принял Model AI Governance Framework, предусматривающий гибкий подход к регулированию ИИ с учётом его конкретного применения. Этот документ получил широкое признание в качестве образца регулирования, адаптивного к быстро меняющимся технологиям.

Важным результатом стало принятие Генеральной Ассамблеей ООН в сентябре 2024 года Глобального цифрового договора (Global Digital Compact), который устанавливает международные стандарты для цифрового управления и защиты цифровых прав. Этот документ подчёркивает необходимость баланса между инновациями и защитой прав человека в цифровой среде.

На межпарламентском уровне была разработана инициатива Межпарламентской Ассамблеей государств – участников СНГ, которая приняла Модельный закон «О цифровых правах» (Постановление МПА № 55-12 от 14 апреля 2023 года). Закон определяет смарт-контракт как «основанный на заранее сформированном алгоритме действий способ заключения соглашения, позволяющий автоматически обеспечить и исполнить обязательство в информационной системе, а в случаях, установленных в правилах информационной системы, – также разрешить возникший спор, установить юридические факты или совершить иные действия». Данное определение может служить основой для унификации подходов в пространстве СНГ.

Первым и основополагающим элементом Цифрового кодекса должен служить единый понятийный аппарат, который устранит существующую терминологическую путаницу. Необходимо установить универсальную систему дефиниций, применимых во всех сферах цифрового права и признанных всеми органами государственной власти, судами и правоприменителями [Имгрунт: 130]. Такой аппарат должен включать:

- определение информационных систем, учитывающее их многообразие и функциональное назначение;
- ясные дефиниции цифровых прав, цифровых активов и цифровых товаров;
- определение понятий, связанных с ИИ, включая определение степеней автономности систем;
- унификацию правил, касающихся смарт-контрактов и других программируемых инструментов;
- устранение противоречивости в определении субъектов цифровых отношений.

На фундаменте единого понятийного аппарата должны быть выстроены базовые принципы цифрового права, которые будут направлять применение всех норм кодекса. Технологическая нейтральность означает, что правовые нормы должны быть сформулированы таким образом, чтобы они оставались применимы независимо от конкретной технологии или платформы, на которой они реализуются. Это позволит избежать устаревания законодательства по мере появления новых технологических решений. Принцип открытости и прозрачности алгоритмов предусматривает, что при использовании ИИ-систем для принятия решений, касающихся прав и интересов граждан, должна быть обеспечена возможность понимания основ таких решений и механизмов их принятия [Харитонова: 350]. Это особенно актуально для государственных органов при применении ИИ в сфере правосудия, социального обеспечения и иных значимых сфер.

Защита прав человека в цифровой среде как ключевой принцип предполагает создание механизмов защиты от дискриминации, от неправомерного сбора и использования персональных данных, от алгоритмического манипулирования и иных форм нарушения прав в цифровой среде. Цифровой суверенитет предусматривает право государства устанавливать

собственные правила функционирования цифровой инфраструктуры на его территории, защиту критической информационной инфраструктуры и недопустимость подчинения национальной цифровой среды иностранному политическому влиянию [Усольцев: 149]. Защита данных и конфиденциальности конкретизирует обязанность операторов обеспечивать безопасность персональных данных, минимизировать их сбор и использование только в целях, санкционированных субъектами данных [Алексеева: 238].

Отдельный и существенный раздел Цифрового кодекса должен быть посвящен правовому регулированию ИИ: он определит правовой статус ИИ-систем, установит механизмы ответственности за их решения и закрепит принципы этичного использования. Опыт экспериментального правового регулирования ИИ в Москве может стать важной основой для формирования федеральных норм.

Еще одним критически важным элементом должно стать закрепление правового режима смарт-контрактов. Кодекс должен дать чёткое определение смарт-контракта и установить юридически признанные правила заключения, исполнения и ответственности при нарушении условий смарт-контрактов.

На этапе разработки законопроекта № 419059-7 «О внесении изменений в Федеральный закон «О связи» и иные законодательные акты Российской Федерации в части развития цифровой экономики» было предложено определить смарт-контракт как «договор в электронной форме, исполнение прав и обязательств по которому осуществляется путём совершения в автоматическом порядке цифровых транзакций в распределённом реестре цифровых транзакций». Несмотря на обоснованность этого определения, оно было исключено из финальной версии закона, оставив правовой статус смарт-контрактов в состоянии неопределённости.

Международный опыт демонстрирует различные подходы к этому явлению. В отдельных штатах США (особенно в Вайоминге) смарт-контракты получили статус юридически признанных инструментов, и суды применяют стандартные контрактные доктрины к их рассмотрению [Отабоев: 939]. Закон Blockchain Technology Act штата Иллинойс содержит специальные положения о признании блокчейна и связанных с ним инструментов [Ефимова: 82]. Модельный закон Межпарламентской Ассамблеи СНГ предусматривает детальное регулирование, включая возможность автоматического разрешения споров через ИИ-системы, встроенные в смарт-контракты.

Отдельная глава Цифрового кодекса должна быть посвящена защите прав человека в цифровой среде [Морозова: 1394], включая:

- право на цифровую идентичность (право каждого лица контролировать использование своего имени, образа, голоса и других идентификационных характеристик в цифровой среде, включая право требовать удаления персональных данных) [Sullivan: 723];

- защиту от алгоритмической дискриминации (запрет на использование алгоритмов и ИИ-систем, которые приводят к дискриминации по признакам расы, национальности, пола, возраста, инвалидности или иным защищённым характеристикам) [Wang: 1320277.].

- защиту от дипфейков (установление ответственности за создание и распространение синтетического контента (дипфейков), используемого для клеветы, фальсификации или введения в заблуждение). Примером передового подхода является закон, принятый в Дании для борьбы с дипфейками. Этот закон гарантирует гражданам исключительные права на использование своего образа, голоса и уникальных черт лица в цифровом пространстве и предусматривает строгую ответственность за неправомерное создание и распространение синтетического контента, использующего личную идентификацию лица[7].

Ключевым и, пожалуй, наиболее серьёзным вызовом при создании Цифрового кодекса является принципиальное расхождение между скоростью развития технологий и

инертностью традиционного законодательного процесса. Цифровая среда меняется стремительно – новые технологии появляются и распространяются в течение месяцев или даже недель. В то же время внесение изменений в кодификационный акт требует длительного парламентского процесса, согласований между различными органами власти и заинтересованными сторонами.

Второй значительный вызов состоит в том, что цифровые отношения носят ярко выраженный межотраслевой характер. Они пронизывают гражданское право (контракты, собственность, интеллектуальные права), административное право (государственное управление, лицензирование), уголовное право (киберпреступность), трудовое право (телеработа, использование ИИ в управлении трудом), налоговое право (определение налоговой базы цифровых платформ) и другие отрасли. Создание специализированного «Цифрового кодекса» порождает сложность в определении чётких границ его предмета регулирования. Кодекс не должен превращаться ни в источник пробелов (там, где его нормы не охватывают какой-то аспект цифровых отношений), ни в источник конфликтов норм (когда норма кодекса противоречит нормам других отраслей).

Третий вызов связан с глобальной, трансграничной природой цифровой среды. Разработка Цифрового кодекса требует внимательного учёта растущего массива международных стандартов, саморегулирования в сфере интернета (ICANN – Internet Corporation for Assigned Names and Numbers, IETF – Internet Engineering Task Force и иные организации) и обеспечения совместимости с зарубежным законодательством. Одновременно крайне важно сохранить национальный цифровой суверенитет и не допустить прямого переноса чуждых правовых моделей, разработанных для условий иных государств.

Четвёртый вызов вытекает из того, что реализация проекта Цифрового кодекса неминуемо породит комплексные коллизии с актуальным законодательством, которое развивалось спонтанно и содержит множество специальных норм, регулирующих отдельные аспекты цифровой среды.

Пятый, идеологический вызов вытекает из обоснованного скептицизма, существующего в научной среде относительно самой целесообразности создания Цифрового кодекса. Как отмечает известный специалист по цифровому праву М.А. Рожкова, существует аргументированное мнение «об отсутствии необходимости в создании Цифрового кодекса, поскольку не получится закрепить все нормы цифрового права в одном кодификационном акте» [Рожкова: 3]. Эта критика основана на наблюдении, что цифровые отношения характеризуются высокой динамичностью, множественностью форм и постоянным появлением новых явлений, которые невозможно полностью предусмотреть в едином кодексе.

Интеграция технологий ИИ в судебные системы стала глобальной тенденцией, демонстрирующей практическую необходимость создания адекватного правового регулирования [Володин: 86].

В Эстонии используются ИИ-алгоритмы для автоматизации рассмотрения мелких исков, включая споры по потребительским кредитам. Система анализирует информацию по делу, формирует проекты судебных решений и предоставляет их судье для утверждения. Эта практика показала возможность разгрузить судебную систему от рутинной работы при сохранении контроля судей над результатами.

В Китае функционирует система «умных судов» (smart courts), где ИИ используется практически при вынесении каждого вердикта. Система проверяет наличие ссылок на соответствующие законы и НПА, разрабатывает проекты юридических документов, выявляет ошибки и иные проблемы судебных постановлений. Такой подход позволил значительно повысить качество и консистентность судебных решений.

В Германии ИИ-системы используются для систематизации процессуальных алгоритмов, анализа, создания и архивирования текстов судебных решений, а также для управления и распределения накопившихся дел по очередности рассмотрения [Черепанова: 4884]. Это позволило повысить эффективность работы судов и снизить сроки рассмотрения дел.

В России процесс цифровизации правосудия идёт более медленными темпами, но пребывает в фазе интенсивного развития. По данным статистики на 2024 год, объём подаваемых в электронном виде документов в арбитражные суды вырос в 20,5 раза по сравнению с предыдущими годами[8]. Это свидетельствует о резко возросшем проникновении цифровых инструментов в судебный процесс.

* * * * *

Создание Цифрового кодекса РФ представляет собой амбициозный, многоаспектный проект, направленный на формирование системного и непротиворечивого правового регулирования цифровых отношений. Проведённый анализ ясно демонстрирует, что существующая высокая степень фрагментарности и рассредоточенности законодательства создаёт серьёзные препятствия не только для развития цифровой экономики, но и для адекватной защиты прав и интересов участников цифровых отношений.

Исследование выявило три системные проблемы, обосновывающие необходимость кодификации:

1) Терминологическая неопределённость, приводящая к разночтениям в правоприменении и судебной практике, что снижает предсказуемость юридических последствий для частных лиц и организаций.

2) Технологическое отставание законодательства, при котором такие явления, как генеративный ИИ, NFT, метавселенные и иные инновации остаются вне чёткого правового регулирования, создавая риски для инвесторов и пользователей.

3) Юрисдикционные конфликты в глобальной цифровой среде, где национальные права вступают в противоречие с деятельностью иностранных платформ и международных корпораций, требуя нового подхода к разрешению споров.

При этом перспективы создания кодекса связаны с формированием единого правового пространства, развитием экспериментального регулирования и цифровизацией правоприменительной практики.

Успех проекта Цифрового кодекса будет зависеть от способности законодателя создать гибкий и адаптивный правовой инструмент, способный эффективно регулировать динамично развивающиеся цифровые отношения при сохранении фундаментальных правовых принципов и конституционных гарантий. Реализация концепции Цифрового кодекса может стать важным стратегическим шагом в формировании современной правовой системы, адекватной вызовам цифровой эпохи, которая способна внести значительный вклад в устойчивое развитие российской цифровой экономики, повышение уровня правовой защиты граждан и организаций в цифровой среде и укрепление позиций России как современного государства, адекватно реагирующего на вызовы информационного века.

Примечания

[1] Цифровой кодекс: как будет выглядеть новая концепция регулирования ИКТ // ПАО Сбербанк: сайт. 2024, 23 мая. URL: https://sber.pro/publication/tsifrovoi-kodeks-kak-budet-viglyadet-novaya-kontseptsiya-regulirovaniya-ikt/ (дата обращения: 10.10.2025).

[2] Как LegalTech-технологии помогают юристам в работе // Лигал Академия: сайт. 2023, 3 августа. URL: https://legalacademy.ru/sphere/post/kak-legaltech-tehnologii-pomogayut-yuristam-v-rabote (дата обращения: 10.10.2025).

[3] *Афонин А.* Google оспорил российский штраф на 2 ундециллиона рублей // Газета.Ру: инф. сайт.

2025, 23 января. URL: https://www.gazeta.ru/tech/news/2025/01/23/24904952.shtml (дата обращения: 10.10.2025).

[4] Минцифры планирует представить проект Цифрового кодекса в середине 2025 года // Interfax: инф. сайт. 2024, 28 мая. URL: https://www.interfax.ru/russia/962612 (дата обращения: 10.10.2025).

[5] Цифра не дотянула до кодекса // Коммерсантъ: инф. сайт. 2023, 15 декабря. URL: https://www.kommersant.ru/doc/6397720?utm_source=Securitylab.ru (дата обращения: 10.10.2025).

[6] Кыргызская Республика. Законы. Цифровой кодекс Кыргызской Республики: Закон Кыргызской Республики от 31 июля 2025 года № 178 // Министерство Юстиции Кыргызской Республики: офиц. сайт. URL: https://cbd.minjust.gov.kg/3-48/edition/35412/ru (дата обращения: 10.10.2025).

[7] *Jacobs S*. Landmark deepfake law aims to give Denmark's citizens rights over their image, voice, and likeness // TechSpot: website. 2025, June 28. URL: https://www.techspot.com/news/108485-landmark-deepfake-law-aims-give-danish-citizens-legal.html (date of access: 10.10.2025).

[8] 3 из 4 документов подаются в арбитражные суды РФ онлайн через сервис «Мой арбитр» // Правовые новости: инф. сайт. 2024, 24 апреля. URL: https://pravo.ru/news/252757/ (дата обращения: 10.10.2025).

Список литературы

Алексеева Ю.С. Принципы защиты цифрового суверенитета государства // Трансформация механизма государства в период становления и развития инновационного электронного государства: сб. статей. Минск: Белорусский государственный экономический университет, 2024. С. 237-240.

Апт Л.Ф. Основные черты понятийного аппарата информационного законодательства / Л.Ф. Апт, А.Г. Ветров // Правовая информатика. 2018. № 2. С. 65-73.

Володин Е.А. Особенности внедрения искусственного интеллекта в судебные процессы: автоматизация и цифровизация правоприменения // Юридическая наука. 2025. № 4. С. 85-89.

Волос А.А. Цифровые права: некоторые проблемы толкования правил статьи 141.1 Гражданского кодекса Российской Федерации // Банковское право. 2024. № 3. С. 16-23. DOI: 10.18572/1812-3945-2024-3-16-23

Даниленко И.М. Проблемы регулирования цифровых прав в Российской Федерации // Гуманитарный научный вестник. 2024. № 6. С. 82-87. DOI: 10.5281/zenodo.12686039

Джендубаева С.А. Искусственный интеллект и метавселенные: правовое регулирование и перспективы интеграции // Проблемы экономики и юридической практики. 2024. Т. 20, № 3. С. 100-108.

Ефимова Л.Г. Сравнительный анализ доктринальных концепций правового регулирования смарт-контрактов в России и зарубежных странах / Л.Г. Ефимова, И.Е. Михеева, Д.В. Чуб // Право. Журнал Высшей школы экономики. 2020. № 4. С. 79-105. DOI: 10.17323/2072-8166.2020.4.78.105

Жернова В.М. Правовой режим информационных систем: дис. … канд. юрид. наук. Челябинск, 2017. 213 с.

Имгрунт С.И. Правовое регулирование в условиях цифровизации: проблемы и перспективы // Северо-Кавказский юридический вестник. 2022. № 2. С. 129-134. DOI: 10.22394/2074-7306-2022-1-2-129-134

Морозова С.С. Защита прав граждан современной России в цифровую эпоху: политико-правовой анализ / С.С. Морозова, Ю.Г. Смирнова // Креативная экономика. 2024. Т. 18, № 6. С. 1375-1394. DOI: 10.18334/ce.18.6.121082

Отабоев Н.О. Смарт контракты в электронном правительстве // Экономика и социум. 2023. № 6-1(109). С. 937-942.

Павлова Д.А. Цифровые права как объект частноправового регулирования: дис. … канд. юрид. наук. Санкт-Петербург, 2025. 210 с.

Полежаев О.А. Личные неимущественные права автора в контексте NFT: проблемы юридической квалификации и новая парадигма // Журнал Суда по интеллектуальным правам. 2024. № 4(46). С. 196-201. DOI: 10.58741/23134852_2024_4_17

Рожкова М.А. Является ли цифровое право отраслью права и ожидать ли появления цифрового кодекса? // Хозяйство и право. 2020. № 4(519). С. 3-12.

Ситников М.С. Право и метавселенная: некоторые вопросы теории и практики // Цифровое право. 2023. Т. 4, № 3. С. 51-71. DOI: 10.38044/2686-9136-2023-4-3-2

Усольцев А.Е. Концептуальные основы и принципы Цифрового кодекса России // Молодой ученый.

2025. № 36(587). С. 149-152.

Харитонова Ю.С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 337-358. DOI: 10.21202/jdtl.2023.14

Черепанова А.С. Цифровизация судебных процессов: опыт различных стран // Научный аспект. 2024. Т. 36, № 5. С. 4882-4887.

Sullivan C. Digital identity – From emergent legal concept to new reality // Computer Law & Security Review. 2018. Vol. 34, № 4. P. 723-731.

Wang X. Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices / X. Wang, Y.C. Wu, X. Ji, H. Fu // Frontiers in Artificial Intelligence. 2024. Vol. 7. P. 1320277.

Law

Alexander K. KOZHEVNIKOV

master's degree, Ural Institute of Management – branch of RANEPA under the President of the Russian Federation (Yekaterinburg, Russia),
Alex_kozh00@mail.ru

DIGITAL CODE OF THE RUSSIAN FEDERATION: LEGAL CHALLENGES AND PROSPECTS

Scientific adviser:
Artem V. Mazein
Reviewer:
Ekaterina Kovrigina
Paper submitted on: 10/10/2025;
Accepted on: 12/15/2025;
Published online on: 12/15/2025.

Abstract. The article examines current challenges related to the creation of the Digital Code of the Russian Federation as a comprehensive legislative framework for regulating digital relations. It issues arising from the modernization of legal regulation in the digital era and assesses the prospects for establishing a unified legal space in the field of information technology. The study employs comparative legal analysis, a systematic approach, legal modeling techniques, and a review of judicial practice and law enforcement experience. As a result, the paper identifies key areas for the advancement of digital legislation and proposes potential solutions to existing legal conflicts.

Keywords: digital code, digital law, digitization, information law, digital rights, artificial intelligence, blockchain, smart contracts, legal regulation

For citation: Kozhevnikov, A. K. Digital Code of the Russian Federation: Legal Challenges and Prospects. StudArctic Forum. 2025, 10 (4): 110–122.

References

Alekseeva Yu.S. Principles of protecting the digital sovereignty of the state. *Transformation of the state mechanism during the formation and development of an innovative electronic state: Collection of articles.* Minsk, Belarusian State Economic University, 2024, pp. 237-240. (In Russ.)

Apt L.F., Vetrov A.G. The main features of the conceptual framework of information technology laws. *Legal Informatics*, 2018, No. 2, pp. 65-73. (In Russ.)

Volodin E.A. Features of the introduction of artificial intelligence in lawsuits: automation and digitalization of law enforcement. *Legal Science*, 2025, No. 4, pp. 85-89. (In Russ.)

Volos A.A. Digital rights: certain problems of interpretation of provisions of Article 141.1 of the Civil Code of the Russian Federation. *Banking Law*, 2024, No. 3, pp. 16-23. DOI 10.18572/1812-3945-2024-3-16-23 (In Russ.)

Danilenko I.M. Problems of regulation of digital rights in the Russian Federation. *Humanitarian Scientific Bulletin*, 2024, No. 6, pp. 82-87. DOI 10.5281/zenodo.12686039 (In Russ.)

Dzhendubaeva S.A. Artificial intelligence and metaverses: Legal regulation and prospects for integration.

Economic Problems and Legal Practice, 2024, Vol. 20, No. 3, pp. 100-108. (In Russ.)

Efimova L.G., Mikheeva I.E, et al. Comparative analysis of doctrinal concepts of legal regulating smart contracts in Russia and foreign states. *Law. Journal of the Higher School of Economics* , 2020, No. 4, pp. 79-105. DOI 10.17323/2072-8166.2020.4.78.105 (In Russ.)

Zhernova V.M. *Legal regime of information systems* . Candidate's thesis (Law). Chelyabinsk, 2017, 213 p. (In Russ.)

Imgrunt S.I. Legal regulation in the context of digitalization: Problems and prospects. *North Caucasus Legal Vestnik*, 2022, No. 2, pp. 129-134. DOI 10.22394/2074-7306-2022-1-2-129-134 (In Russ.)

Morozova S.S., Smirnova Yu.G. Protecting citizens' rights in modern Russia in the digital age: political and legal analysis. *Creative Economy*, 2024, Vol. 18, No. 6, pp. 1375-1394. DOI 10.18334/ce.18.6.121082 (In Russ.)

Otaboev N.O. Smart contracts in electronic government. *Economics and Society*, 2023, No. 6-1(109), pp. 937-942. (In Russ.)

Pavlova D.A. *Digital rights as an object of private law regulation* . Candidate's thesis (Law). St. Petersburg, 2025, 210 p. (In Russ.)

Polezhaev O.A. Personal non-property rights of the author in the context of NFT: problems of legal qualification and a new paradigm. *Zhurnal Suda po intellektual'nym pravam*, 2024, No. 4(46), pp. 196-201. DOI 10.58741/23134852_2024_4_17 (In Russ.)

Rozhkova M.A. Is digital law a branch of law, and should we expect the emergence of a digital code? *Economy and Law*, 2020, No. 4(519), pp. 3-12. (In Russ.)

Sitnikov M.S. Law and the Metaverse: Selected issues in theory and practice. *Digital Law Journal*, 2023, Vol. 4, No. 3, pp. 51-71. DOI 10.38044/2686-9136-2023-4-3-2 (In Russ.)

Usoltsev A.E. Conceptual foundations and principles of the Russian Digital Code. *Young Scientist*, 2025, No. 36(587), pp. 149-152. (In Russ.)

Kharitonova Yu.S. Legal means of providing the principle of transparency of the artificial intelligence. *Journal of Digital Technologies and Law* , 2023, Vol. 1, No. 2, pp. 337-358. DOI 10.21202/jdtl.2023.14 (In Russ.)

Cherepanova A.S. Digitization of court proceedings: Experience of different countries. *Nauchniy aspekt*, 2024, Vol. 36, No. 5, pp. 4882-4887. (In Russ.)

Sullivan C. Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, 2018, Vol. 34, No. 4, pp. 723-731.

Wang X., Wu Y.C., et al. Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. *Frontiers in Artificial Intelligence*, 2024, Vol. 7, p. 1320277.