

DOI 10.31483/r-168815

*Селезнёв Андрей Владимирович**Рак Игорь Петрович**Стрельникова Анастасия Александровна*

**МЕХАНИЗМЫ ЗАЩИТЫ ПРАВ СУБЪЕКТОВ
В ЦИФРОВОЙ ЭКОСИСТЕМЕ:
ПРАВОВЫЕ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ АСПЕКТЫ**

***Аннотация:** в главе рассматривается проблема защищённости прав субъектов в цифровой экосистеме – среде, организованной вокруг платформы, где место традиционного контрагента занимает многостороннее технологическое образование. Показана нераздельность социально-экономических и правовых аспектов: асимметрия информации и переговорной силы, сетевые эффекты, lock-in и алгоритмическое опосредование обесценивают инструменты, рассчитанные на двусторонние отношения. Методологическую основу составили системный и функциональный подходы, формально-юридический и сравнительно-правовой анализ, а также правовое моделирование. Результатом стала четырёхуровневая модель защиты (нормативный, институциональный, процессуально-юрисдикционный и технолого-правовой уровни), расположенные по мере роста специализации и автоматизации. Выявлены барьеры, мешающие реализации прав, – асимметрия информации и переговорной силы, закрытость алгоритмов, трансграничность конфликтов, привязка пользователя к платформе. Обозначены ориентиры совершенствования: приоритет превенции и «защиты по построению», подлинная доступность процедур, обязательная объяснимость алгоритмов, регулирование и сближение международных стандартов.*

***Ключевые слова:** цифровая экосистема, платформенная экономика, защита прав субъектов, асимметрия переговорных возможностей, закрытость алгоритмов, алгоритмическая дискриминация, объяснимость решений, защита данных по построению, привязка к платформе, платформенная занятость, превенция нарушений, четырёхуровневая модель защиты.*

Abstract: *the chapter examines the problem of protecting the rights of subjects in the digital ecosystem – an environment organized around a platform, where traditional counterparties are replaced by a multilateral technological construct. It demonstrates the inseparability of socio-economic and legal aspects: information asymmetry and bargaining power imbalances, network effects, lock-in, and algorithmic mediation devalue instruments designed for bilateral relations. The methodological framework includes systemic and functional approaches, formal-legal and comparative-legal analysis, as well as legal modeling. The result is a four-level protection model (normative, institutional, procedural-jurisdictional, and techno-legal levels), arranged in order of increasing specialization and automation. Barriers hindering the exercise of rights are identified – information asymmetry and bargaining power imbalances, opacity of algorithms, cross-border nature of conflicts, and user lock-in to the platform. Guidelines for improvement are outlined: priority of prevention and "protection by design," genuine accessibility of procedures, mandatory explainability of algorithms, co-regulation, and harmonization of international standards.*

Keywords: *digital ecosystem, platform economy, protection of subjects' rights, bargaining power asymmetry, opacity of algorithms, algorithmic discrimination, algorithmic explainability, privacy by design, lock-in effect, platform employment, prevention of violations, four-level model of protection.*

Введение.

Цифровизация затронула не только отдельные институты, но и саму среду, в которой человек и организация осуществляют свои права. Прежде хозяйственная и социальная жизнь опиралась на двусторонние связи – продавец и покупатель, работодатель и работник, банк и клиент. Теперь между сторонами всё чаще стоит третье: сложное многостороннее образование, выстроенное вокруг платформы, – цифровая экосистема. Отдельная сделка внутри неё уже не самодостаточна. Она вплетена в непрерывный технологический процесс, которым распоряжаются владелец платформы и работающие на его стороне алгоритмы. Текст закона при этом может оставаться неизменным – меняются условия, в которых он реализуется, а

вместе с ними и сама возможность субъекта отстоять нарушенный интерес [21, с. 86].

Главная проблема заключается здесь в том, что право консервативно и медленно, а технологии – нет. Пока законодатель осмысляет одну сложившуюся практику, экосистема порождает несколько новых. Пользователь, принявший условия соглашения одним нажатием, формально наделён внушительным набором прав, однако на пути к их осуществлению встают барьеры технического и организационного свойства. Разрыв между «правом в книгах» и «правом в действии», описанный ещё социологической юриспруденцией, в цифровой среде обретает не теоретическое, а вполне осязаемое, массовое измерение [20, с. 6].

Цель работы раскрывается в определении средств защиты прав субъекта в цифровой экосистеме и демонстрации нераздельности её экономической и правовой сторон. Требуется уточнить само понятие цифровой экосистемы и очертить состав её участников, а также выяснить, какие экономические силы одних субъектов ослабляют, а другим дают перевес. Разрозненные защитные инструменты необходимо собрать в систему и оценить, где проходят пределы её эффективности.

Методологическую базу составили анализ и синтез, системный и функциональный подходы, формально-юридический и сравнительно-правовой методы. Особо выделим правовое моделирование: именно оно позволило свести множество частных приёмов защиты к компактной конструкции из четырёх уровней. Новизна подхода не в том, чтобы изобрести новые права. Она в смене угла зрения. Защищённость субъекта мы оцениваем не по тому, записана ли в законе соответствующая норма, а по тому, может ли конкретный человек в конкретных обстоятельствах реально до этой защиты «дотянуться». Как отмечает А.Я. Матунов, категория «экосистема» в конкурентном праве только формируется и требует осмысления именно с позиций фактической зависимости участников [17].

1. Понятие и структура цифровой экосистемы как среды реализации прав.

Термин «экосистема» право заимствовало у биологии и теории управления. Заимствование оказалось точным: оно схватывает главное – перед нами не арифметическая сумма участников, а взаимозависимое сообщество, живущее за счёт общей инфраструктуры. В цифровом контексте под новой экосистемой мы понимаем организованную вокруг платформы среду, где производство, обмен и потребление благ идут через программно-алгоритмические средства, а поведение участников удерживают в рамках сразу три регулятора – закон, договор и технические алгоритмы. Одна деталь здесь принципиальна: владелец платформы и участвует в отношениях, и устанавливает их правила.

Устроена среда послойно. Внизу – инфраструктура: серверы, сети, хранилища. Выше – платформа, которая сводит спрос с предложением и исполняет сделки. Особый слой образуют данные; сведения о поведении пользователей здесь не побочный продукт, а самостоятельный актив. На вершине – доступные пользователю сервисы. Нарушение права возможно на любом уровне, и сбой внизу нередко отзывается наверху. Р.И. Васиян подчёркивает, что юридическая природа цифровой экосистемы до сих пор не получила устойчивой правовой идентификации, что затрудняет применение традиционных конструкций [13].

Цифровая экосистема – это базирующаяся на одной (или более) цифровой платформе качественно специфическая среда в сфере экономики, в которой посредством взаимодействующих между собой технических средств, информационных технологий и сервисов осуществляются связи между её субъектами, для которых, таким образом, создаются различные продукты и услуги, дополнительно обеспечивающие им организационные удобства, финансовую привлекательность и другие ценности. При всей безусловной тесной взаимосвязи понятий платформы и экосистемы их нельзя отождествлять: цифровые экосистемы выступают лишь следующей фазой развития цифровых платформ и могут включать в себя несколько цифровых платформ.

Экономику платформ держит сетевой эффект: чем больше участников, тем ценнее площадка для каждого. Однако, собрав критическую массу пользователей, площадка получает возможность диктовать условия доступа, и формально

добровольное согласие превращается в присоединение к предложенному – без реального выбора. Перед нами классическая проблема слабой стороны договора, лишь перенесённая в новые технологические условия.

Экосистемы неоднородны. Одни строятся на разовых транзакциях: маркетплейс (тот же Wildberries или Ozon) свёл покупателя с продавцом – и его роль исчерпана. Другие удерживают пользователя постоянно, сращивая десятки сервисов в единое «суперприложение» – так работают экосистемы Яндекса и Сбера, где одна учётная запись открывает платежи, доставку, транспорт и общение. Чем теснее интеграция, тем глубже зависимость субъекта и тем выше цена вопроса о защите: покинуть отдельный маркетплейс проще, а выход из экосистемы, охватывающей значительную часть цифровой активности, оказывается практически невозможным. А. Н. Гулемин, анализируя национальные и международные подходы, отмечает, что единого рецепта защиты не существует – он обязан считаться и с типом площадки, и с глубиной вовлечённости субъекта [14].

Ещё одна определяющая черта – алгоритмическое опосредование. Что показать выше в выдаче, кому отказать в доступе, какую цену назначить, какой контент удалить – эти решения принимает не сотрудник, а программная модель. Трудность в том, что её логика скрыта не только для пользователя, но нередко и для самого оператора. Как оспорить решение, оснований которого не видно? Как доказать дискриминацию, если её механизм упрятан в параметры нейронной сети? Наконец, цифровая экосистема почти всегда трансгранична. Инфраструктура – в одной стране, оператор зарегистрирован в другой, данные хранятся в третьей, пользователь находится в четвёртой. Отсюда споры о применимом праве и компетентном органе; отсюда же «правовой арбитраж». Без международного сотрудничества защита в таких условиях неизбежно остаётся половинчатой.

2. Субъектный состав цифровой экосистемы и особенности правового положения его участников.

Защита начинается с определения того, кого защищают. В цифровой экосистеме вопрос осложнён подвижностью ролей: один и тот же субъект за короткое время успевает побыть покупателем, продавцом, автором отзыва и поставщиком

данных для рекламной системы. И всё же для юридического анализа участников допустимо свести к нескольким типам.

Первый тип – операторы, владельцы платформенной инфраструктуры, устанавливающие правила. Положение их двойственно: по форме это рядовые участники оборота, по существу – носители публично значимой функции организатора среды. Второй тип – бизнес-пользователи, предприниматели, для которых платформа стала каналом выхода на рынок и оттого источником зависимости. Третий – конечные пользователи, потребители. Есть и четвёртый: поставщики данных, сторонние разработчики, а также лица, чьи права нарушены опосредованно, вовсе без договора с платформой [2, ст. 2].

Объединяет столь разных участников одно – глубокая асимметрия. На одной стороне оператор: за ним информационное, технологическое, организационное превосходство, он пишет договор присоединения, видит поведение каждого пользователя, в любой момент вправе переменить функциональность сервиса. На другой – пользователь, которому остаётся принять предложенное, ибо реальной альтернативы нет. Такая модель взаимодействия приводит к тому, что принцип свободы договора реализуется лишь формально, тогда как его содержательная сторона оказывается существенно ограниченной. Продавец вынужден присоединяться к условиям, которые в полной мере отражают интересы маркетплейса как более сильной стороны, контролирующей инфраструктуру, доступ к аудитории и механизмы продвижения товара. Эта изначальная неравновесность и оправдывает особые, компенсирующие механизмы защиты – по той же логике, по какой право некогда встало на сторону потребителя в споре с продавцом [3, ст. 16]. Н.А. Булгакова указывает на коллизии интересов продавцов и потребителей именно в экосистемах маркетплейсов, где оператор одновременно организует рынок и конкурирует с участниками [12].

Вопрос об искусственном интеллекте требует отдельного рассмотрения. Автоматизированные системы субъектами права не являются и в обозримом будущем едва ли станут. Однако их решения порождают вполне реальные последствия для людей. Значит, принцип должен быть закреплён твёрдо: за действия

алгоритма отвечает тот, кому он принадлежит и кто его эксплуатирует, а за человеком сохраняется право на пересмотр значимого решения – с участием другого человека.

Таблица 1

Субъекты цифровой экосистемы и типичные угрозы их правам

Категория субъекта	Основной интерес	Типичные угрозы правам
Оператор экосистемы	Устойчивость платформы, доход	Регуляторные ограничения, ответственность за действия третьих лиц
Бизнес-пользователь	Доступ к рынку и клиентам	Одностороннее изменение условий, дискриминационное ранжирование, «блокировка»
Конечный пользователь (потребитель)	Качество и безопасность услуги	Навязанные условия, неправомерная обработка данных, непрозрачные решения
Поставщик данных/разработчик	Признание вклада, вознаграждение	Присвоение результатов, ограничение совместимости
Опосредованно затронутое лицо	Неприкосновенность частной сферы	Обработка данных без согласия, репутационный вред

Предварительный анализ таблицы выявляет неравномерное распределение рисков: их концентрация наблюдается в группе зависимых участников – бизнес-пользователей и потребителей. Можно сделать вывод, что защиту следует строить компенсаторно, выравнивая то фактическое неравенство, которое рынок сам по себе не устраняет.

3. Социально-экономические предпосылки формирования механизмов защиты прав.

Любой защитный механизм обусловлен экономическими причинами. Он рождается из определённых условий рынка и обслуживает вполне определённые интересы, а потому оценивать его в отрыве от этих условий бессмысленно. Норма начинает действовать не в тот момент, когда её удачно сформулировали, а тогда, когда она совпадает с реальной расстановкой стимулов у сторон.

Первое, с чего приходится начинать, – данные. Сведения о запросах, покупках, перемещениях и контактах пользователя стали активом, вокруг которого выстраиваются целые бизнес-модели. Экономика подталкивает собирать их как

можно шире; право ставит встречный предел – сбор оправдан лишь в объёме, необходимом и соразмерном заявленной цели [5, ст. 5]. Интерес тут не только частный. Скопление данных в одних руках задевает и конкуренцию, и национальную безопасность.

Вторая предпосылка – структурное неравенство. Экономия на масштабе, сетевые эффекты, контроль над данными дают оператору устойчивый перевес, который рынок сам не размывает. Показательно, что и зарубежный законодатель признаёт нужду в особом регулировании доминирующих платформ: по Регламенту ЕС о цифровых рынках Европейская комиссия присвоила крупнейшим цифровым компаниям, таким как Amazon, Apple, ByteDance (TikTok), Microsoft и другим, статус «привратников» (gatekeepers), возложив на них дополнительные обязанности под угрозой штрафа до 10% общемирового оборота [22]. В российской практике экосистемы Яндекс, VK, МТС иллюстрируют ту же концентрацию: единый идентификатор связывает поиск, транспорт, финансы и медиа, повышая стоимость выхода для пользователя. Социальный смысл защитных механизмов в том и состоит, чтобы вернуть переговорным весам хотя бы минимальное равновесие.

Есть предпосылка менее осязаемая, но по значимости не уступающая прочим, – доверие. Субъект включается в экосистемные отношения ровно настолько, насколько верит в добросовестность оператора и в возможность защиты. На языке экономики доверие – социальный капитал цифровой среды.

Особого освещения заслуживает платформенная занятость. Курьеры, водители, исполнители на цифровых биржах – по разным оценкам, около 2,8 млн россиян постоянно получают доход через приложения [21]. Формально многие сохраняют статус самозанятых [6], по существу же подчиняются алгоритму: он раздаёт заказы, считает рейтинг, в одностороннем порядке способен отключить исполнителя от сервиса. Трудо-правовые гарантии на них, как правило, не распространяются. Этот разрыв не остался незамеченным судами. Всё чаще они исходят из того, что содержание отношений важнее их оформления, и переквалифици-

руют договоры с самозанятыми в трудовые [16]. Законодатель отреагировал: Федеральный закон от 31 июля 2025 г. №289-ФЗ «Об отдельных вопросах регулирования платформенной экономики», вступающий в силу 1 октября 2026 г., вводит фигуры оператора платформы и партнёра-исполнителя, учреждает реестр посреднических цифровых платформ и задаёт базовые правила их взаимодействия [11]. Насколько эти правила защитят самих исполнителей, покажет практика.

Нельзя сбрасывать со счетов и цифровое неравенство. Доступ к технологиям и умение ими пользоваться распределены крайне неравно. Пожилой человек или житель отдалённой местности зачастую не представляет ни объёма отдаваемых данных, ни сути принимаемых обязательств. Право обязано подстраховать его: презумпциями в его пользу, требованием излагать условия внятным языком, защитой, что действует по умолчанию. Последняя предпосылка связана со скоростью. Цифровые процессы стремительны, а их сбои масштабируемы: одно ошибочное правило бьёт разом по сотням тысяч. Акцент смещается с восстановления на предупреждение.

4. Система правовых механизмов защиты прав субъектов в цифровой экосистеме.

Одним средством в цифровой экосистеме не обойтись. Нужна система, охватывающая содержание прав, порядок их осуществления и восстановление после нарушения. Предлагаемая нами конструкция насчитывает четыре уровня, представленных по нарастанию специализации и автоматизации: нормативный, институциональный, процессуально-юрисдикционный, технолого-правовой. Схематически она изображена на рисунке 1.



Рис. 1. Четырёхуровневая модель механизмов защиты прав субъектов
в цифровой экосистеме

4.1. Нормативно-правовые механизмы.

В основании всей конструкции лежат нормы: они определяют, чем субъект вправе располагать и где проходит предел дозволенного для оператора. Выше прочего стоят конституционные гарантии – неприкосновенность частной жизни, тайна переписки, свобода информации, защита от произвольного вмешательства [1, ст. 23, 24]. Это ценностный каркас, обязательный для любого отраслевого акта и в конечном счёте для условий каждого пользовательского соглашения.

Следующий пласт – отраслевое законодательство: гражданское, административное, специальное информационное. Гражданско-правовой инструментарий позволяет оспорить кабальную сделку, взыскать убытки, добиться компенсации морального вреда. Административный – привлечь оператора к ответственности, прежде всего за небрежное обращение с персональными данными [4, ст. 13.11]. В этой части подход законодателя заметно ужесточился. С 30 мая 2025 г. действует Федеральный закон от 30 ноября 2024 г. №420-ФЗ, который ввёл за утечки оборотные штрафы: повторное нарушение обходится компании в 1–3% годовой выручки [10]. Массив законов об информации и о персональных данных описывает режим работы со сведениями и наделяет субъекта осязаемыми

правомочиями – знать, что о нём собрано, добиваться исправления, удаления, отзыва согласия [5]. Здесь же – конструкция цифровых прав, появившаяся в Гражданском кодексе в 2019 г., а вслед за ней и легализованные цифровые финансовые активы [9].

Заметное место на нормативном уровне занимают экспериментальные правовые режимы. Они дают опробовать регулирование новинки на ограниченном участке, не подвергая риску всех сразу [8]. Постепенно складывается и отдельный контур для искусственного интеллекта. Рамку задаёт Национальная стратегия развития ИИ до 2030 года [7]; рядом с ней действует и добровольный Кодекс этики в сфере ИИ. Отечественная модель пока держится мягкого, рамочного подхода и сознательно расходится с жёсткой архитектурой европейского Регламента об ИИ.

4.2. Институциональные механизмы.

Норма без органа, следящего за её соблюдением, остаётся пожеланием. Второй уровень образуют институты: регуляторы и надзорные органы, уполномоченные по правам, а также структуры внутри самой экосистемы – от службы поддержки до механизмов саморегулирования. Их дело – контроль, разбор обращений, пресечение нарушений на ранней стадии.

Заметная тенденция последних лет – возложение на операторов публично значимых обязанностей: раскрывать условия, объяснять свои решения, обеспечивать их обжалование. Платформа перестаёт быть нейтральным посредником и становится ответственной за порядок на организуемой ею территории. Регламент ЕС о цифровых услугах прямо требует от крупных платформ оценивать системные риски и заводить внутренние процедуры рассмотрения жалоб [23, ст. 20]; отечественное регулирование движется в ту же сторону – в частности, через ужесточение административной ответственности и институт оборотных штрафов. На этом же уровне вызревают институты доверия – независимая сертификация, аудит алгоритмов. Их польза в том, что они отчасти восполняют информационный дефицит слабой стороны.

4.3. Процессуально-юрисдикционные механизмы.

Третий уровень отвечает на вопрос, что делать, когда право уже нарушено. Здесь и судебная защита, и внесудебные пути – претензия, медиация, системы онлайн-урегулирования. Суд остаётся универсальной гарантией, но в цифровой среде он сталкивается с препятствиями: нарушение технической природы трудно доказать, оператор нередко находится в чужой юрисдикции, а издержки процесса перекрывают цену требования.

Показателен массовый тип спора, выросший вокруг маркетплейсов. Типичная фабула: площадка в одностороннем порядке блокирует личный кабинет продавца, ссылаясь на нарушение внутренних правил, и замораживает причитающиеся выплаты. Проблема усугубляется отсутствием прозрачной и формализованной процедуры обжалования решений о блокировке. В действующей системе взаимоотношений между маркетплейсом и продавцами не предусмотрено действенных механизмов оперативного восстановления доступа к платформе, что ставит предпринимателей, особенно представителей малого и микробизнеса, в заведомо уязвимое положение [13].

Суды в подобных делах вынуждены оценивать соразмерность санкции и добросовестность оператора; с 1 октября 2026 г. опору для них создаст Закон о платформенной экономике, впервые регламентирующий основания блокировки и порядок её обжалования [11]. Оттого растёт значение внесудебных механизмов, встроенных в саму платформу. Онлайн-урегулирование разбирает типовые конфликты быстро и почти без затрат. Отдельную трудность создаёт доказывание: нарушение мимолётно, страница изменена, запись стёрта. Возрастает роль средств фиксации электронных следов. Общее правило, по которому доказывает истец, в отношениях с оператором стоит смягчить. Не мало важно сказать и о коллективных формах: если решение оператора негативно сказывается на большой группе, эффективнее объединить требования.

5. Технологическо-правовые механизмы защиты.

Самое примечательное в цифровой защите прав – механизмы, где юридическое требование исполняет не человек и не суд, а техника. Традиционный инструмент включается постфактум, когда вред уже нанесён. Технолого-правовой встроен в архитектуру системы и потому способен нарушение предотвратить.

Ведущий принцип уровня – защита данных на этапе проектирования и по умолчанию (или «privacy by design and by default»). Суть его в том, чтобы думать о правах субъекта не после запуска продукта, а с первой строки технического задания, и чтобы самые щадящие для пользователя настройки стояли исходно [24, ст. 25]. Так защита превращается из обещания в свойство системы. Второй элемент – информационная безопасность. Без неё любые юридические гарантии остаются пустым звуком. Триада «конфиденциальность – целостность – доступность» принадлежит не одной лишь технике, но и праву.

Третья составляющая – прозрачность и объяснимость алгоритмов; так право отвечает на проблему «чёрного ящика». Ведение журналов, фиксация логики, внятное для человека изложение оснований решения превращают возможность обжалования из декларации в действующий механизм. Особенно это важно там, где решается судьба человека, – доступ к кредиту, к работе, к услуге. Для таких случаев ключевой становится схема «человек в контуре»: последнее слово оставляют не модели, а человеку [19, с. 96].

Отдельного анализа требует алгоритмическая дискриминация – систематическое ущемление отдельных групп, возникающее не из злого умысла, а из данных и внутренней логики модели. Динамическое ценообразование способно предлагать разным пользователям разную цену за идентичный товар. Кредитный или поведенческий скоринг рискует отказывать по признакам, которые прямо не названы, но статистически коррелируют с полом, возрастом или национальностью. Доказать подобное в суде непросто, однако технически возможно: на помощь приходят метрики справедливости, парное тестирование и анализ значимости признаков.

Нельзя пройти мимо смарт-контрактов – программ, которые исполняют условия сделки сами, без посредника. При благоприятном раскладе это самозащита в чистом виде. Но у автоматизма есть слабое звено – оракулы, внешние источники данных. Стоит оракулу передать неверные сведения, и безупречный код исполнит ошибочное решение; кто отвечает в этом случае – право пока внятно не говорит. Наконец, к уровню относится саморегулирование – кодексы, стандарты, внутренние процедуры. Гибкость – несомненный плюс; обратная сторона – склонность вырождаться в формальность. Оттого предпочтительнее модель со-регулирувания. Д.Ш. Исаев, исследуя эволюцию подхода Европейского Союза, показывает, что модель со-управления цифровыми экосистемами становится теоретико-правовым ориентиром и для отечественной доктрины [15].

Таблица 2

Уровни механизмов защиты прав, их направленность и ограничения

Уровень	Основные инструменты	Направленность	Ограничения эффективности и риски
Нормативно-правовой	Конституционные гарантии, отраслевое и специальное законодательство, экспериментальные режимы	Определение объёма прав и границ поведения	Отставание от технологий, декларативность норм, пробелы в регулировании ИИ
Институциональный	Регуляторы, уполномоченные органы, обязанности операторов, институты доверия	Контроль соблюдения и рассмотрение обращений	Дефицит компетенций и ресурсов надзора, риск формального подхода
Процессуально-юрисдикционный	Судебная защита, медиация, онлайн-урегулирование, коллективные иски	Восстановление нарушенного права	Высокие издержки, сложность доказывания, трансграничность споров
Технологическо-правовой	Privacy by design, кибербезопасность, объяснимость алгоритмов, со-регулирование	Превентивная защита «по построению»	Дороговизна аудита и внедрения – барьер для малого и среднего бизнеса

Анализ таблицы позволяет сделать ключевой вывод: уровни не находятся в конкурентных отношениях – они обеспечивают взаимную поддержку и устойчивость системы. Нижние наполняют защиту содержанием, верхние придают ей

скорость и предупредительность. Порознь ни один полной защищённости не даёт; она рождается лишь на их стыке.

6. Проблемы и риски реализации защитных механизмов.

Первый и самый коварный – асимметрия информации и силы. Права субъекту вроде бы даны, а воспользоваться он ими не в состоянии: то не знает о них, то знает, но не понимает, как применить. Право, доступное лишь специалисту, защитной функции для рядового пользователя не несёт.

Второй аспект – непрозрачность алгоритмов как самостоятельная помеха правоприменению. Оспорить решение, оснований которого не видишь, объективно тяжело. И даже там, где закон дарует право на объяснение, оператор заслоняется коммерческой тайной.

Третий – трансграничность, из достоинства среды обратившаяся в процессуальную преграду. Отдельно – эффект «блокировки» (lock-in). Формально уйти с платформы никто не мешает; практически уходить некуда и накладно – там остались данные пользователя, его репутация, годами наработанные связи [22, преамбула].

Есть и обратная опасность – избыточное регулирование. Из благого стремления максимально защитить субъекта легко возникает переизбыток требований: они поднимают издержки входа, стесняют небольших участников и в конечном счёте оборачиваются против самого пользователя – сужением выбора. К этой опасности примыкает внутренняя уязвимость предложенной модели: её цена. Независимый аудит алгоритмов, полноценное внедрение спроектированной приватности – всё это требует ресурсов, посильных крупной платформе, но обременительных для малого и среднего ИТ-бизнеса. Возникает парадокс: механизмы, задуманные против доминирования, способны его закрепить. А.Я. Матунов справедливо указывает, что становление категории «цифровая экосистема» в конкурентном праве всё ещё находится на стадии постановки проблемы [17; 18]. И последнее – отставание практики. Норму можно написать безупречно, но, если применяющий её не понимает технологической сути отношений, она либо применяется с ошибкой, либо не применяется вовсе.

7. Направления совершенствования механизмов защиты прав субъектов

Из перечисленных проблем вытекают и пути их решения. Первое и, по нашему убеждению, ключевое – развернуть систему к превенции. Обязательные требования к проектированию, гарантирующие соблюдение прав по умолчанию, гасят нарушение там, где оно зарождается, – в техническом коде. Это и дешевле, и уместнее для среды, где вред разрастается мгновенно.

Второе – сделать защиту действительно доступной, а не доступной на словах. Упростить процедуры. Обязать излагать условия понятным языком. Развить недорогие и быстрые способы урегулирования споров.

Третье – институционализировать прозрачность алгоритмов: обязать операторов документировать логику значимых автоматизированных решений, допускать независимый аудит, обеспечивать участие человека в контуре принятия социально значимых решений. Коммерческую тайну при этом можно уберечь – раскрывая сведения не публично, а доверенному аудитору.

Четвёртое – развивать со-регулирование. Государство устанавливает рамку, отрасль наполняет её стандартами и кодексами, внешний контроль не даёт гибкости обернуться необоснованными послаблениями. Требования разумно дифференцировать по масштабу оператора.

Пятое – международное сотрудничество. Экосистемы не знают границ, и защита не должна останавливаться на них.

Шестое, без чего прочие меры теряют силу, – грамотность: правовая и цифровая подготовка пользователей и особая квалификация тех, кто нормы применяет. Полезным шагом видится включение в вузовские программы междисциплинарных модулей «цифровой гигиены и IT-права».

Заключение.

Подведём итог. Новая цифровая экосистема – не улучшенный рынок, а качественно иная среда: многосторонняя, с доминирующим оператором-организатором, опосредованная алгоритмом, не признающая границ. Привычные средства защиты, скроенные под отношения двоих, в ней действуют лишь отчасти, а порой не действуют вовсе.

Ответом на этот вызов служит только система – четыре уровня механизмов, каждый со своей ролью. Нормы определяют, что защищать. Институты следят, чтобы защищали. Процессуальные средства восстанавливают нарушенное. Технологические – не дают нарушить, вплетая защиту в само устройство систем. По отдельности они бессильны; вместе складываются в целостную систему, обеспечивающую защищённость субъекта – при условии, что её требования соразмерны и не превращаются в барьер для добросовестных участников.

Критерием эффективности правовой системы выступает не объём нормативного массива, а доступность защиты для рядового гражданина в типичной жизненной ситуации. Этим и заданы приоритеты – превенция вместо запоздалого восстановления, реальная доступность вместо декларируемой, прозрачность вместо «чёрного ящика», со-регулирование вместо крайностей, международная гармонизация вместо юрисдикционной разноголосицы и, поверх всего, грамотность пользователей. Ключевая задача права – сохранить баланс между защитой человека, здоровой конкуренцией и пространством для новых решений.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с изм., одобр. в ходе общероссийского голосования 01.07.2020). – URL: <http://pravo.gov.ru> (дата обращения: 01.08.2026).
2. Федеральный закон «Гражданский кодекс Российской Федерации (часть первая)» №51-ФЗ от 30.11.1994 (ред. от 10.06.2026) // Собрание законодательства РФ. – 1994. – №32. – Ст. 3301.
3. Закон РФ «О защите прав потребителей» №2300–1 от 07.02.1992 (ред. от 28.12.2025, с изм. от 17.02.2026) // Собрание законодательства РФ. – 1996. – №3. – Ст. 140.
4. Федеральный закон «Кодекс Российской Федерации об административных правонарушениях» №195-ФЗ от 30.12.2001 (ред. от 04.07.2026) // Собрание законодательства РФ. – 2002. – №1 (ч. 1). – Ст. 1.

5. Федеральный закон «О персональных данных» №152-ФЗ от 27.07.2006 (ред. от 26.07.2026) // Собрание законодательства РФ. – 2006. – №31 (ч. 1). – Ст. 3451.

6. Федеральный закон «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» №422-ФЗ от 27.11.2018 (ред. от 28.11.2025) // Собрание законодательства РФ. – 2018. – №49 (ч. 1). – Ст. 7494.

7. Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» №490 от 10.10.2019 (ред. от 15.02.2024) (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // Собрание законодательства РФ. – 2019. – №41. – Ст. 5700.

8. Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» №258-ФЗ от 31.07.2020 (ред. от 26.06.2026) // Собрание законодательства РФ. – 2020. – №31 (ч. 1). – Ст. 5017.

9. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» №259-ФЗ от 31.07.2020 (ред. от 15.12.2025) // Собрание законодательства РФ. – 2020. – №31 (ч. 1). – Ст. 5018.

10. Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» №420-ФЗ от 30.11.2024 (ред. от 23.05.2025). – URL: <http://pravo.gov.ru> (дата обращения: 01.08.2026).

11. Федеральный закон «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» №289-ФЗ от 31.07.2025.

12. Булгакова Н.А. Защита прав продавцов и потребителей в экосистемах маркетплейсов: коллизии интересов / Н.А. Булгакова // Образование и право. – 2026. – №4. – С. 104–110. DOI 10.24412/2076-1503-2026-4-104-110. EDN GGOHFT

13. Васиян Р.И. Понятие и юридическая природа цифровой экосистемы: актуальные проблемы правовой идентификации / Р.И. Васиян // Образование и

право. – 2026. – №2. – С. 230–237. DOI 10.24412/2076-1503-2026-2-230-237. EDN VIIFHT

14. Гулемин А.Н. Цифровые экосистемы в современном праве: анализ национальных и международных подходов / А.Н. Гулемин // Электронное приложение к Российскому юридическому журналу. – 2024. – №5. – С. 27–36. DOI 10.34076/22196838_2024_5_27. EDN FRXLBV

15. Исаев Д.Ш. Платформенное право и модель соуправления цифровыми экосистемами: теоретико-правовой анализ эволюции подхода Европейского Союза / Д.Ш. Исаев // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. – 2025. – №12. – С. 130–134. DOI 10.37882/2223-2974.2025.12.13. EDN WJHZEM

16. Киселева Е.В. К вопросу о признании судами трудовых отношений с гражданами, оформленными как самозанятые / Е.В. Киселева // Арбитражный и гражданский процесс. – 2024. – №2. – С. 23–27. DOI 10.18572/1812-383X-2024-2-23-27. EDN KTGUNM

17. Матунов А.Я. Категория «экосистема» в конкурентном праве (постановка проблемы) / А.Я. Матунов // Российское конкурентное право и экономика. – 2026. – №1(45). – С. 32–37. EDN UYARHK

18. Матунов А.Я. Цифровая экосистема: становление новой категории конкурентного права / А.Я. Матунов // Российское конкурентное право и экономика. – 2024. – №4(40). – С. 14–19. DOI 10.47361/2542-0259-2024-4-40-14-19. EDN AQEGLU

19. Понкин И.В. Искусственный интеллект с точки зрения права / И.В. Понкин, А.И. Редькина // Вестник Российского университета дружбы народов. Серия: Юридические науки. – 2018. – Т. 22. №1. – С. 91–109. DOI 10.22363/2313-2337-2018-22-1-91-109. EDN YVXKVA

20. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы / Э.В. Талапина // Журнал российского права. – 2018. – №2(254). – С. 5–17. DOI 10.12737/art_2018_2_1. EDN YNJEIF

21. Хабриева Т.Я. Право в условиях цифровой реальности / Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. – 2018. – №1(253). – С. 85–102. DOI 10.12737/art_2018_1_7. EDN YKWEZL

22. Digital Markets Act: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector // Official Journal of the European Union. – 2022. – L 265. – P. 1–66.

23. Digital Services Act: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services // Official Journal of the European Union. – 2022. – L 277. – P. 1–102.

24. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88.

Селезнев Андрей Владимирович – канд. техн. наук, доцент кафедры «Уголовное право и прикладная информатика в юриспруденции», ФГБОУ ВО «Тамбовский государственный технический университет», г. Тамбов, Россия.

Рак Игорь Петрович – канд. пед. наук, доцент кафедры «Уголовное право и прикладная информатика в юриспруденции», ФГБОУ ВО «Тамбовский государственный технический университет», г. Тамбов, Россия.

Стрельникова Анастасия Александровна – студентка кафедры «Уголовное право и прикладная информатика в юриспруденции», ФГБОУ ВО «Тамбовский государственный технический университет», г. Тамбов, Россия.
