

Замечания к проекту федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации»

I. ПЕРВООЧЕРЕДНЫЕ ПРИНЦИПИАЛЬНЫЕ ЗАМЕЧАНИЯ

1. Вся полнота регулирования по ключевым вопросам фактически делегирована Правительству РФ

Одна из главных проблем законопроекта состоит в том, что он не закрепляет на уровне федерального закона значительную часть реально существенных правил, а передает их определение Правительству РФ, уполномоченным органам и ведомствам. В результате сам закон оказывается рамочным, а его наиболее значимые последствия для граждан, бизнеса, образования и государственного управления будут определяться не парламентом, а будущими подзаконными актами.

Подобный подход особенно опасен потому, что именно на подзаконный уровень выносятся не второстепенные технические детали, а ключевые элементы всей модели регулирования. Иными словами, закон не отвечает на самые важные вопросы, а лишь создает конструкцию, внутри которой они будут решаться позднее, административным путем.

Ниже перечислены ключевые вопросы, которые проект фактически отдает на усмотрение Правительства и ведомств.

- **Критерии доверенных моделей.** Именно критерии доверенных моделей будут определять, какие ИИ-решения вообще смогут применяться в государственных системах и на значимых объектах. Однако сами критерии не закреплены в законе. Это создает риск того, что доступ к наиболее чувствительным сегментам рынка будет зависеть не от ясных и публично обсужденных норм, а от подзаконных требований, содержание которых может меняться и формироваться под влияние сильнейших игроков.
- **Порядок включения в реестр.** Процедура включения в реестр — это фактически механизм допуска на стратегический рынок. Если она не детализирована в самом законе, появляется риск непрозрачных административных барьеров, затягивания сроков, избирательного подхода и создания преимуществ для тех, кто лучше встроен во взаимодействие с регулятором.
- **Требования к безопасности.** Безопасность ИИ — центральный элемент регулирования, особенно при использовании в государственном управлении, образовании, социальной сфере и критической инфраструктуре. Однако закон не закрепляет, что именно понимается под безопасностью, какие технические испытания обязательны, какие виды рисков должны проверяться и каким образом будет подтверждаться соответствие.
- **Требования к качеству.** Понятие качества в отношении ИИ должно опираться на прозрачные и измеримые критерии. Но проект оставляет это на усмотрение отраслевых органов и иных структур. Это опасно, поскольку качество может начать определяться произвольно, несопоставимо между сферами и без единых стандартов проверки.
- **Случаи обязательного применения отдельных моделей.** Закон допускает, что Правительство будет определять случаи обязательного использования доверенных

моделей на отдельных объектах. Это означает, что административным актом может быть навязано применение ИИ в важнейших сферах без прямого решения законодателя и без полноценного обсуждения рисков.

- **Порядок маркировки.** Вопрос маркировки синтезированного контента крайне чувствителен для информационной безопасности, борьбы с мошенничеством и защиты граждан от дипфейков. Но вместо четкого регулирования в законе предлагается подзаконный порядок, который может оказаться либо избыточно формальным, либо слишком слабым.
- **Отдельные параметры прав граждан.** Право на отказ, на информирование, на обжалование, на доступ к неавтоматизированному рассмотрению не должны зависеть от административного усмотрения. Тем не менее значимая часть этих механизмов в проекте либо не раскрыта, либо предполагает последующее уточнение Правительством.
- **Иные условия допуска и использования ИИ.** Такая размытая формулировка открывает возможность в дальнейшем вводить практически любые дополнительные требования, ограничения и исключения на подзаконном уровне, не возвращаясь к полноценной законодательной процедуре.

Все это означает, что наиболее спорные вопросы — включая потенциальный допуск ИИ в образование, социальную сферу, государственное управление, инфраструктурные контуры и иные чувствительные области — могут быть решены без должного общественного и экспертного обсуждения. Для граждан это означает снижение гарантий прав и предсказуемости. Для бизнеса — невозможность долгосрочного планирования. Для общества — подмену законодательного регулирования административным.

Негативные последствия:

- **Подмена закона подзаконным регулированием.** Формально будет существовать федеральный закон, но реальные правила игры будут устанавливаться постановлениями, приказами и ведомственными актами. Это снижает качество правового регулирования и ослабляет парламентский контроль.
- **Рост административного усмотрения.** Чем больше существенных вопросов не урегулировано в законе, тем больше зависит от чиновника, ведомства или правительства. Это создает почву для непрозрачности, избирательного подхода и конфликтов интересов.
- **Ослабление общественного обсуждения.** Подзаконные акты принимаются в ином режиме, чем федеральные законы, и не проходят такого же уровня публичного, научного и парламентского обсуждения. Это особенно опасно для решений, затрагивающих детей, образование и права граждан.
- **Правовая нестабильность.** Если ключевые правила вынесены из закона, они могут меняться чаще и быстрее. Участники рынка и граждане будут жить в режиме постоянной неопределенности.
- **Создание предпосылок для лоббизма.** Чем меньше определенности в законе, тем больше значение приобретает влияние на подзаконное нормотворчество. Это усиливает позиции крупных игроков и ослабляет независимых участников.

Такая конструкция ПФЗ требует проверки на соответствие статьям 18, 46 и 55 Конституции Российской Федерации и принципу правовой определенности, выработанному в практике Конституционного Суда РФ, поскольку существенные вопросы реализации прав граждан, допуска технологий в чувствительные сферы и ограничения возможных форм поведения не могут быть в неопределенном объеме переданы на подзаконный уровень.

2. Нормы об ответственности разработчиков, операторов и владельцев сервисов ИИ прописаны декларативно и могут сделать фактическое привлечение виновных невозможным

Вторая фундаментальная проблема проекта — слабость и декларативность положений об ответственности. Законопроект заявляет, что субъекты отношений в сфере ИИ несут ответственность за результат, нарушающий законодательство, но не создает работающего механизма распределения такой ответственности. В тексте отсутствуют ясные критерии того, где именно проходит граница между ответственностью разработчика модели, интегратора, владельца сервиса, оператора системы и конечного пользователя.

Особую проблему создает то, что проект использует крайне неопределенные категории — например, “результат, полученный с использованием искусственного интеллекта”, “должны были знать”, “исчерпывающие меры”, “соразмерно степени вины”. Без специальной детализации эти формулы звучат строго, но на практике они могут оказаться почти неприменимыми. В области ИИ, где результат часто вероятностный, зависит от данных, настроек, промптов, контекста, внешней интеграции и условий эксплуатации, расплывчатые общие слова не заменяют четкого правового механизма.

Чтобы ответственность в такой сфере работала, закон должен четко отвечать на вопросы:

- что считается дефектом модели;
- что считается дефектом эксплуатации;
- какие действия доказывают достаточную осмотрительность разработчика;
- какие обязанности по мониторингу и логированию лежат на операторе;
- когда пользователь выходит за пределы обычного использования;
- кто отвечает за вред, причиненный при интеграции модели в конкретный прикладной контур;
- какие доказательства должны храниться и представляться в споре.

Ничего этого в проекте нет в должной степени. Декларативность норм об ответственности требует оценки с точки зрения статей 45 и 46 Конституции РФ, а также согласованности с положениями Гражданского кодекса РФ об общих основаниях возмещения вреда (в частности, статья 1064 ГК РФ), поскольку без ясного распределения ролей и стандартов осмотрительности защита пострадавшего лица может оказаться неэффективной.

Негативные последствия:

- **Перекалывание ответственности по цепочке.** Разработчик будет ссылаться на неправильную эксплуатацию, оператор — на свойства модели, владелец сервиса — на действия пользователя, а пользователь — на логику системы. В результате установить виновного будет крайне трудно.

- **Фактическая незащищенность пострадавшего.** Гражданин, столкнувшийся с ущербом, будет вынужден разбираться в сложной технологической цепочке, не имея доступа к журналам, архитектуре модели, внутренним ограничениям и распределению ролей между участниками.
- **Правовая неопределенность для добросовестных участников.** Независимые разработчики и малый бизнес не смогут заранее понять пределы своей ответственности. Это будет отпугивать новых игроков и сдерживать развитие отрасли.
- **Избирательное правоприменение.** При отсутствии ясных критериев ответственность может определяться не по объективным правилам, а по административной логике, политической конъюнктуре или ресурсам сторон.
- **Снижение стимулов к реальной безопасности.** Если закон не устанавливает конкретных стандартов осмотрительности и доказуемых процедур, участники рынка будут ориентироваться не на безопасность, а на формальное прикрытие рисков.

3. Законопроект внутренне противоречив: он декларирует опору на традиционные духовно-нравственные ценности, но одновременно создает основу для технократического вытеснения человеческого нравственного суждения

Проект провозглашает в числе принципов регулирования учет и уважение традиционных российских духовно-нравственных ценностей. Однако сама архитектура закона допускает расширение применения ИИ в сферах, где решения затрагивают честь, достоинство, развитие, правовое положение, благополучие и судьбу человека. Это принципиально противоречивая конструкция.

Искусственный интеллект по своей природе является инструментом вычисления, обработки данных, статистического вывода, классификации и прогнозирования. Он не обладает:

- совестью;
- милосердием;
- нравственной ответственностью;
- способностью к покаянию;
- способностью к человеческому состраданию;
- внутренним моральным выбором.

Даже самый совершенный ИИ не является субъектом нравственной ответственности. Он не может различать человеческую трагедию и просто аномалию в данных. Он не способен к живому пониманию контекста так, как способен человек, несущий перед другим человеком моральную и правовую ответственность. Поэтому алгоритмический вывод не должен становиться основанием для принятия решений в тех сферах, где требуется не только формальная рациональность, но и человеческое нравственное суждение.

Расширение возможностей применения ИИ в сферах, затрагивающих судьбу человека, требует оценки на соответствие статьям 2, 18 и 21 Конституции РФ, а также Указу Президента РФ от 09.11.2022 № 809 и Стратегии национальной безопасности РФ, поскольку алгоритмический вывод не может подменять человеческое нравственное и ответственное суждение там, где

затрагиваются достоинство личности, воспитание, социальная поддержка и иные фундаментальные блага.

Это особенно важно для:

- образования;
- правоохранительной деятельности;
- судебной и квазисудебной сферы;
- социальной поддержки;
- работы с семьями, детьми, инвалидами, пожилыми;
- сфер, где решается вопрос о доступе к помощи, ограничениях, санкциях, характеристиках личности и поведении человека.

Негативные последствия:

- **Подмена совестного решения цифровым выводом.** Там, где раньше требовались ответственность, разум, опыт и нравственная оценка должностного лица, может появиться соблазн прикрыться “нейтральным решением системы”.
- **Обесчеловечивание управления.** Чем больше значимые решения зависят от ИИ, тем выше риск, что человек будет рассматриваться не как личность, а как набор цифровых признаков и вероятностных оценок.
- **Рост несправедливых решений.** Алгоритм не знает ни милосердия, ни исключительности жизненной ситуации, ни человеческой ошибки как предмета прощения или понимания. Это делает особенно опасным его влияние в судьбоносных сферах.
- **Противоречие заявленным ценностям.** Формально ценности провозглашаются, но фактически они вытесняются технократической логикой. Это подрывает доверие к самому закону.
- **Размывание личной ответственности должностных лиц.** При широком внедрении ИИ в чувствительные сферы всегда возникает риск, что чиновник, педагог, администратор или иной субъект начнет оправдывать свое решение ссылкой на алгоритм.

4. В проекте отсутствует специальное регулирование применения ИИ в образовании, что создает прямую угрозу детям, педагогике и самой сути образовательного процесса

Один из самых опасных пробелов законопроекта — почти полное отсутствие специального режима для образования. Между тем образовательная среда не является обычным рынком цифровых услуг. Здесь речь идет не просто о потреблении технологии, а о формировании личности, мышления, памяти, внимания, ценностей, навыков общения и способности к самостоятельному суждению. Любое внедрение ИИ в образование без специальных гарантий затрагивает не только техническую, но и культурную, психологическую и цивилизационную основу общества.

Если в законе нет специальных ограничений, это означает, что ИИ-системы могут внедряться в школы, колледжи, вузы и иные образовательные организации:

- без обязательной педагогической экспертизы;

- без психологической экспертизы;
- без этической экспертизы;
- без доказанной безопасности для когнитивного развития;
- без долгосрочной оценки влияния на память, внимание, мотивацию, самостоятельность, письмо, мышление и речь.

Это особенно опасно в отношении детей и подростков, чья психика и когнитивные функции находятся в стадии формирования. Для них ИИ — не просто удобный цифровой инструмент, а фактор, который может менять структуру учебного процесса, сокращать объем самостоятельной умственной работы, ослаблять способность к сосредоточению и формировать зависимость от машинной подсказки.

Отсутствие специального режима для образования требует проверки на соответствие статьям 21, 38 и 43 Конституции РФ, Федеральному закону № 273-ФЗ «Об образовании в Российской Федерации» и Федеральному закону № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», поскольку внедрение ИИ в образовательный процесс без специальных гарантий может затронуть достоинство обучающегося, безопасность образовательной среды и право ребенка на развитие.

Негативные последствия:

- **Превращение образования в полигон технологических экспериментов.** Школа и вуз могут стать средой, где новые ИИ-решения будут внедряться до того, как изучено их реальное влияние на обучающихся.
- **Ослабление когнитивного развития.** При бесконтрольном использовании ИИ есть риск снижения самостоятельности мышления, ухудшения навыков письма, анализа, поиска аргументов и удержания внимания.
- **Деградация роли педагога.** Вместо живого наставничества и педагогической ответственности может усиливаться технократическая модель, где педагог превращается в обслуживающий элемент цифровой платформы.
- **Подмена образования цифровым обслуживанием.** Если обучение будет строиться вокруг автоматизированных подсказок, оценки и рекомендаций, то сама идея образования как формирования личности окажется под угрозой.
- **Рост неравенства.** Школы и вузы с разным уровнем ресурсов будут получать разные по качеству ИИ-инструменты, что усилит образовательный разрыв и зависимость от коммерческих платформ.

5. В законопроекте необходимо прямо закрепить специальные образовательные гарантии: запрет распознавания эмоций, обязательную экспертизу и особый режим данных несовершеннолетних

Если законопроект вообще будет дорабатываться, в нем обязательно должны появиться специальные защитные механизмы для образования. Эти механизмы не могут оставаться на уровне рекомендаций, локальных актов школы или ведомственных писем. Они должны быть закреплены непосредственно в законе, поскольку речь идет о правах детей, роли семьи,

достоинстве личности и допустимых пределах цифрового воздействия в воспитательной и образовательной среде.

5.1. Запрет на применение систем ИИ для распознавания эмоций в образовательных организациях

Системы распознавания эмоций не должны использоваться в школах, колледжах, вузах и иных образовательных организациях. Такие технологии строятся на крайне спорных предпосылках о возможности по мимике, голосу, микродвижениям, темпу речи или иным сигналам достоверно судить о внутреннем состоянии человека. В реальности они дают высокий риск ложных интерпретаций, культурных и поведенческих искажений, стигматизации и грубого вторжения в личное пространство.

Для ребенка или подростка это особенно опасно. В образовательной среде система, которая “считывает эмоции”, неизбежно превращается в инструмент психологического наблюдения. Она может маркировать ученика как “нелояльного”, “тревожного”, “агрессивного”, “пассивного”, “неуспешного”, “неудобного” или “подозрительного” на основе сомнительной машинной интерпретации. Это несовместимо с уважением достоинства личности и с базовыми принципами педагогики.

Использование систем распознавания эмоций и расширенная обработка образовательных данных несовершеннолетних без специального правового режима требуют оценки на соответствие статьям 21, 23 и 24 Конституции РФ, положениям Федерального закона № 152-ФЗ «О персональных данных», а также гарантиям защиты прав ребенка, поскольку затрагивают частную жизнь, достоинство личности и чувствительную информацию о несовершеннолетних.

Негативные последствия:

- нормализация цифрового психологического контроля над детьми;
- стигматизация обучающихся по ложным или сомнительным признакам;
- разрушение доверительной образовательной среды;
- вмешательство в внутренний мир ребенка;
- создание опасной практики скрытого поведенческого мониторинга.

5.2. Обязательная педагогическая, психологическая и этическая экспертиза ИИ-инструментов до их внедрения

Любой ИИ-инструмент, который предполагается использовать в образовательном процессе, должен проходить обязательную независимую экспертизу. Недостаточно проверять только техническую работоспособность или информационную безопасность. Необходимо заранее оценивать:

- влияние на когнитивное развитие;
- влияние на мотивацию к обучению;
- влияние на самостоятельность;
- влияние на психологическое состояние;
- влияние на отношения ученик–учитель;

- влияние на образовательное неравенство;
- влияние на воспитательную среду.

Без такой экспертизы образовательные учреждения становятся зависимыми от маркетинга поставщиков и административного давления на цифровизацию. Педагогика не может подчиняться логике “сначала внедрим, потом посмотрим”. В отношении детей и молодежи такая логика недопустима.

Негативные последствия:

- внедрение вредных или недоисследованных решений;
- разрушение учебных практик, доказавших свою эффективность;
- навязывание школам и вузам ИИ-инструментов без доказанной пользы;
- усиление коммерческого влияния на образовательную политику;
- снижение качества образования под видом технологической модернизации.

5.3. Особый режим обработки образовательных данных несовершеннолетних

Образовательные данные ребенка — это не просто техническая информация. К ним относятся:

- академические результаты;
- траектория обучения;
- поведенческие особенности;
- психологические характеристики;
- сведения о затруднениях, интересах и особенностях развития;
- данные об успеваемости, участии, дисциплине и взаимодействии с педагогами.

Такие данные являются чувствительными и в совокупности могут формировать глубокий цифровой профиль несовершеннолетнего. Поэтому в законе должен быть закреплён особый режим их обработки.

- **Запрет на использование образовательных данных в коммерческих целях.** Школа и вуз не должны становиться источником сырья для платформенного бизнеса. Информация о ребенке не должна превращаться в коммерческий актив.
- **Запрет на использование таких данных для дообучения моделей без обезличивания.** Даже если данные собираются в рамках образовательного процесса, это не означает автоматического права использовать их для совершенствования ИИ-моделей.
- **Необходимость согласия в установленной форме.** Любое использование данных несовершеннолетних сверх прямых образовательных целей должно быть подчинено специальным и строгим требованиям к информированному согласию.
- **Особые требования к хранению, доступу, передаче и удалению.** Чем чувствительнее данные, тем строже должны быть правила их жизненного цикла.

Негативные последствия при отсутствии этих гарантий:

- формирование цифровых досье на детей;
- коммерциализация образовательной информации;
- неконтролируемое дообучение ИИ на детских данных;
- повышенный риск утечек и злоупотреблений;
- долговременный вред правам ребенка, репутации и будущему социальному положению.

II. ДОПОЛНИТЕЛЬНЫЕ СИСТЕМНЫЕ ЗАМЕЧАНИЯ

6. Базовые понятия законопроекта размыты, противоречивы и непригодны для устойчивого правоприменения

Проект одновременно вводит понятия “искусственный интеллект”, “система искусственного интеллекта”, “сервис искусственного интеллекта”, “технологии искусственного интеллекта”, “модель искусственного интеллекта”, но не выстраивает между ними ясной и непротиворечивой логики. Частично они дублируют друг друга, частично пересекаются, а в ряде случаев используются так, будто сами авторы закона не определились, что именно является основным объектом регулирования.

Это не терминологическая мелочь, а фундаментальный дефект конструкции закона. Если закон не различает объект разработки, объект эксплуатации, пользовательский сервис, модель как вычислительный объект и систему как интегрированное прикладное решение, то невозможно четко распределить:

- обязанности;
- требования безопасности;
- порядок допуска;
- границы ответственности;
- права граждан;
- особенности аудита и контроля.

Например, одни нормы адресуются модели, другие — сервису, третьи — технологиям, четвертые — системе. Но без четкого разграничения невозможно понять, какие обязанности относятся к базовой модели, какие — к прикладной оболочке, какие — к оператору внедренного решения, а какие — к конечному владельцу продукта.

Размытость базовых понятий законопроекта требует оценки с точки зрения конституционного принципа правовой определенности, вытекающего из статей 15, 17, 18 и 19 Конституции РФ и подтвержденного в практике Конституционного Суда РФ, поскольку неясность объекта регулирования неизбежно ведет к произвольному толкованию обязанностей, ограничений и ответственности.

Негативные последствия:

- **Хаотичное правоприменение.** Органы власти, суды и участники рынка будут по-разному толковать одни и те же положения, что породит нестабильность и конфликты.

- **Избирательное давление.** Размытые категории удобны для расширительного толкования против одних участников и мягкого толкования в пользу других.
- **Невозможность заранее планировать деятельность.** Бизнес и разработчики не смогут понять, какие именно нормы на них распространяются и в каком объеме.
- **Проблемы в судебной защите.** При споре о вреде, обязанности или нарушении закона стороны будут прежде всего спорить о том, что именно регулировалось законом — модель, система, сервис или технология.
- **Низкое качество закона как источника права.** Чем хуже базовые определения, тем слабее весь последующий механизм регулирования.

7. Законопроект декларирует безопасность, но не содержит реальных технических стандартов безопасного ИИ

Проект многократно ссылается на безопасность, но фактически не раскрывает, в чем именно должна выражаться безопасность ИИ-систем. В современном контексте безопасность ИИ — это не просто защита информации в традиционном смысле. Это также:

- устойчивость к манипуляциям входными данными;
- защита от adversarial-атак;
- защита от jailbreak и обхода ограничений;
- устойчивость к prompt injection;
- предотвращение data poisoning;
- защита от извлечения модели и утечек обучающих данных;
- контроль галлюцинаций и недостоверных выводов;
- проверка поведения системы в нестандартных сценариях;
- отслеживание дрейфа модели после внедрения.

Ничего этого закон в явном виде не требует. Не установлены единые обязательные процедуры:

- технического тестирования;
- независимого аудита;
- журналирования;
- оценки обновлений модели;
- red teaming;
- инцидент-репортинга;
- процедуры отзыва или приостановки использования при обнаружении опасного поведения.

В итоге создается иллюзия строгого подхода к безопасности при фактическом отсутствии его содержательного наполнения.

Декларативный характер требований к безопасности требует оценки на соответствие статьям 41 и 45 Конституции РФ, Федеральному закону № 149-ФЗ и, применительно к значимым объектам, Федеральному закону № 187-ФЗ, поскольку отсутствие специальных технических стандартов безопасного ИИ создает риск формального, а не реального обеспечения безопасности личности, организаций и инфраструктуры.

Негативные последствия:

- **Формальная, а не реальная безопасность.** Система может быть “доверенной” по документам, но небезопасной по своему фактическому поведению.
- **Рост числа инцидентов.** Без обязательных технических проверок повышается риск ошибок, утечек, обхода защит и вредоносного использования.
- **Ложное чувство защищенности.** Государство, организации и граждане будут считать систему безопасной только потому, что она прошла формальную процедуру допуска.
- **Недостаточная готовность к реальным угрозам.** Современные риски ИИ не сводятся к классической информационной безопасности, а проект регулирует их крайне поверхностно.
- **Высокие последствия ошибок в чувствительных сферах.** Если такие системы окажутся в образовании, госуправлении или КИИ, цена инцидента будет многократно выше.

8. Реестр “доверенных моделей” создает риск административной монополизации и вытеснения независимых разработчиков

Идея отдельного режима допуска к государственным системам сама по себе может обсуждаться, но в предложенном виде механизм “доверенных моделей” слишком тесно связан с административным усмотрением. Если критерии доверенности, порядок включения, порядок проверки и условия обязательного применения выносятся на подзаконный уровень, реестр становится не только инструментом безопасности, но и инструментом перераспределения рынка.

В таких условиях выигрывает не обязательно лучший технологический продукт, а тот, кто:

- обладает крупными ресурсами;
- способен проходить сложные бюрократические процедуры;
- имеет устойчивые каналы взаимодействия с регуляторами;
- может позволить себе дорогостоящие согласования, экспертизы и инфраструктурные издержки.

Малые и средние компании, исследовательские команды, университетские лаборатории и независимые разработчики в такой конструкции почти неизбежно оказываются в неравном положении.

Конструкция реестра доверенных моделей в сочетании с широким подзаконным усмотрением требует оценки на соответствие статьям 8 и 34 Конституции РФ и Федеральному закону № 135-ФЗ «О защите конкуренции», поскольку способна привести к созданию административных барьеров входа, дискриминации независимых участников рынка и концентрации доступа к стратегическим сегментам у ограниченного круга игроков.

Негативные последствия:

- **Снижение конкуренции.** Чем выше административный барьер входа, тем меньше реальных участников способно выйти на рынок значимых ИИ-решений.
- **Рост монополизации.** Рынок государственных и окологосударственных ИИ-сервисов будет концентрироваться вокруг узкого круга крупных игроков.
- **Падение стимулов к инновациям.** Если успех зависит прежде всего от допуска в реестр, а не от качества решения, у участников снижается мотивация к реальному технологическому прорыву.
- **Зависимость государства от ограниченного круга поставщиков.** Это опасно и экономически, и с точки зрения устойчивости инфраструктуры.
- **Удорожание решений.** Снижение конкуренции ведет к росту цены и ухудшению условий для заказчика, в том числе государственного.

9. Конструкция “суверенных” и “национальных” моделей оторвана от реальности современной разработки ИИ

Современная разработка ИИ — это глобальная кооперация. Она включает:

- открытые фреймворки;
- международные библиотеки;
- модели и веса open source;
- распределенные команды;
- трансграничные научные публикации;
- открытые датасеты и инструменты.

В этом контексте требование, чтобы все стадии разработки, обучения и эксплуатации модели происходили исключительно на территории РФ и исключительно российскими лицами, выглядит либо технически и организационно невыполнимым, либо резко сужающим круг потенциальных участников рынка.

Фактически такая конструкция не столько создает суверенитет, сколько вводит искусственный барьер против реальной научно-технологической среды, в которой сегодня развивается ИИ. Суверенитет в высоких технологиях достигается не запретом на международную кооперацию как таковую, а способностью создавать собственные конкурентоспособные решения, пользуясь лучшими доступными инструментами, знаниями и инфраструктурами.

Чрезмерно широкая возможность ограничивать трансграничные ИИ-решения требует оценки на соответствие статьям 29, 34 и 44 Конституции РФ, поскольку может затронуть свободу получения информации, предпринимательскую деятельность, научное и техническое творчество и создать несоразмерные барьеры для развития отечественной науки и высокотехнологичного бизнеса.

Негативные последствия:

- **Дискриминация открытой науки и open source.** Использование глобальных библиотек, фреймворков и открытых моделей может оказаться фактически вытеснено из “правильного” правового режима.

- **Замыкание на ограниченном внутреннем контуре.** Вместо технологической самостоятельности может возникнуть изоляция от реальной мировой экосистемы разработки.
- **Потеря доступа к мировой экосистеме разработки.** Это затронет и научные коллективы, и коммерческие команды, и образовательные программы.
- **Снижение темпов прогресса.** Искусственная изоляция почти всегда замедляет развитие, особенно в столь динамичной сфере.
- **Превращение “суверенитета” в самоизоляцию.** В результате страна рискует отстать еще сильнее, прикрывая это отставание формальным языком независимости.

10. Возможность ограничения или запрета трансграничных ИИ-решений нанесет удар по науке, бизнесу и кадрам

Положения о трансграничных технологиях ИИ в текущем виде открывают путь к ограничению или запрету значимой части зарубежных платформ и решений. Формально это может подаваться как защита суверенитета, но на практике для современной ИИ-отрасли доступ к передовым мировым инструментам является не роскошью, а частью профессиональной среды.

Сегодня обучение специалистов, научные исследования, стартапы, прикладные интеграции, корпоративные продукты и образовательные программы часто строятся с использованием лучших доступных глобальных решений. Ограничение такого доступа ударяет не только по “пользовательскому удобству”, но и по всей экосистеме:

- исследователям становится сложнее работать на мировом уровне;
- предприниматели теряют ключевые технологические компоненты;
- преподаватели и студенты лишаются современных инструментов;
- команды начинают искать юрисдикции с более предсказуемым режимом.

Если передовые решения будут ограничены, а взамен рынок будет вынужден использовать менее конкурентоспособные аналоги только потому, что они доступны внутри административно защищенного контура, это резко ухудшит позиции России в глобальной технологической гонке.

Недостаточная определенность прав граждан на информирование, отказ, получение объяснения и эффективное обжалование требует оценки на соответствие статьям 18, 21, 24, 45 и 46 Конституции РФ, поскольку без ясных гарантий человек оказывается в уязвимом положении перед непрозрачными автоматизированными процедурами, способными затрагивать его права и законные интересы.

Негативные последствия:

- **Отставание по качеству технологий.** Без доступа к сильнейшим мировым решениям разрыв будет только увеличиваться.
- **Разрушение существующих бизнес-моделей.** Многие компании уже строят продукты поверх иностранных API, библиотек и платформ.
- **Утечка кадров.** Специалисты будут уезжать туда, где они могут работать с лучшими инструментами и не сталкиваться с искусственными ограничениями.

- **Ослабление науки и образования.** Университеты и исследовательские центры будут выпадать из глобальной профессиональной среды.
- **Рост издержек на внутреннем рынке.** Ограничение конкуренции снаружи почти всегда ведет к росту цены и снижению качества внутри.

11. Формально закрепленные права граждан остаются слабыми, неполными и во многом декларативными

Законопроект формально говорит об информировании граждан о применении ИИ, о возможности уведомления при автономных решениях и о досудебном обжаловании. Однако эти положения не образуют полноценного и реально работающего режима защиты. В тексте отсутствуют ясные ответы на вопросы:

- в каких случаях гражданин вправе отказаться от применения ИИ;
- кто обязан обеспечить такой отказ;
- какова процедура выражения отказа;
- в каких сферах отказ обязателен;
- когда гражданин имеет право на решение человека;
- в какой форме он должен получить объяснение;
- кто и как обязан это объяснение предоставить.

Особенно тревожно то, что право на отказ от использования ИИ поставлено в зависимость от случаев, которые в дальнейшем установит Правительство. Это означает, что право существует как абстрактная декларация, но его реальный объем определяется не самим законом.

Отсутствие прямых и развернутых запретов на манипулятивное и профилирующее использование ИИ требует оценки на соответствие статьям 19, 21, 23, 24 и 29 Конституции РФ, поскольку подобные практики затрагивают достоинство личности, автономию воли, частную жизнь и могут вести к скрытому ограничению свободы выбора.

Негативные последствия:

- **Фиктивность права на отказ.** Гражданин может быть формально уведомлен о применении ИИ, но фактически не иметь возможности выбрать человеческое рассмотрение.
- **Невозможность понять решение.** Без права на объяснение и прозрачного описания логики системы человек не сможет эффективно защитить свои права.
- **Ослабление досудебной защиты.** Обжалование без доступа к основаниям решения часто превращается в формальность.
- **Рост цифрового принуждения.** ИИ может стать навязанным посредником в доступе к услугам, правам и возможностям.
- **Удар по уязвимым группам.** Пожилые, малообеспеченные, цифрово неграмотные граждане и семьи с детьми окажутся в наиболее слабом положении.

12. Законопроект не вводит полноценной защиты от манипулятивного, профилирующего и поведенчески воздействующего использования ИИ

Современные ИИ-системы способны не только “обрабатывать информацию”, но и влиять на поведение человека через персонализированное воздействие, скрытое профилирование, индивидуализированную подачу контента, подстройку рекомендаций под психологические особенности и эксплуатацию уязвимостей. Закон упоминает эксплуатацию уязвимостей человека, но не создает полноценного специального режима защиты от таких практик.

Между тем реальная опасность ИИ сегодня состоит не только в ошибке, но и в способности незаметно подталкивать человека к нужному для платформы, продавца, работодателя, кредитора или иного субъекта решению. Особенно остро это проявляется в отношении:

- несовершеннолетних;
- пожилых;
- лиц в стрессовом состоянии;
- людей с финансовыми трудностями;
- лиц с психологическими особенностями;
- пользователей, не способных распознать скрытую цифровую манипуляцию.

Лазейки в регулировании маркировки синтетического контента требуют оценки на соответствие статье 29 Конституции РФ, а также нормам гражданского законодательства о защите чести, достоинства и деловой репутации (в частности, статьи 150 и 152 ГК РФ), поскольку недостаточная прозрачность происхождения контента создает риски введения граждан в заблуждение, мошенничества и причинения репутационного вреда.

Негативные последствия:

- **Скрытое управление поведением.** Пользователь будет считать, что действует свободно, тогда как его решение будет технологически направляться.
- **Дискриминационное профилирование.** ИИ сможет относить людей к риск-группам, сегментам или “нежелательным” категориям на основе непрозрачной логики.
- **Усиление эксплуатации уязвимых групп.** Те, кто меньше защищен, станут основной мишенью для манипулятивных цифровых практик.
- **Рост недоверия к цифровой среде.** Если люди почувствуют, что платформы не просто помогают, а скрыто управляют ими, это подорвет доверие ко всей цифровой инфраструктуре.
- **Подмена свободы выбора персонализированным воздействием.** Это противоречит и правам человека, и самой идее уважения автономии личности.

13. Нормы о маркировке синтезированного контента содержат лазейки, фактически подрывающие саму идею прозрачности

Статья о маркировке синтезированного контента могла бы стать важной гарантией информационной прозрачности, однако в текущем виде она содержит опасную лазейку. Возможность предусмотреть соглашением отсутствие обязательности маркировки в формате, воспринимаемом человеком, фактически позволяет владельцу сервиса переложить проблему на пользовательское соглашение.

Это означает, что сервис сможет формально соблюдать закон, а пользователь — “согласиться” на отсутствие видимой маркировки, зачастую даже не осознавая всех последствий такого согласия. В результате значимая защита от скрытой генерации контента обнуляется.

Положения проекта об интеллектуальной собственности требуют проверки на согласованность со статьей 44 Конституции РФ и частью IV Гражданского кодекса РФ, поскольку без специальной и детальной увязки с действующим режимом охраны результатов интеллектуальной деятельности они не устраняют, а закрепляют правовую неопределенность в отношении статуса результатов, созданных с использованием ИИ.

Негативные последствия:

- **Рост дипфейков и скрыто сгенерированного контента.** Если маркировка не будет очевидной для человека, это резко повысит риск злоупотреблений.
- **Удар по репутации граждан.** Немаркированные синтетические аудио, видео и изображения могут использоваться для клеветы, шантажа и дискредитации.
- **Рост мошенничества.** Граждане будут чаще становиться жертвами поддельных голосов, изображений и сообщений.
- **Подрыв доверия к информации.** Чем больше немаркированного синтетического контента, тем меньше доверия к цифровой среде в целом.
- **Фиктивность защиты.** Формально закон будет требовать маркировку, но реально пользователи будут сталкиваться с контентом без понятного предупреждения.

14. Положения об интеллектуальной собственности не решают существующих проблем и лишь создают видимость регулирования

Законопроект касается вопросов интеллектуальной собственности, однако фактически не решает ни одной из базовых проблем генеративного ИИ. Он не дает ясного ответа:

- какова правовая природа результата, созданного при помощи ИИ;
- где граница творческого вклада человека;
- как соотносятся права пользователя, владельца сервиса и разработчика модели;
- как учитываются права авторов материалов, использованных для обучения;
- какие правила действуют при воспроизведении охраняемых элементов в выводе модели.

Простая отсылка к Гражданскому кодексу не решает проблему, потому что действующее регулирование не создавалось под нынешние масштабы генеративных моделей и связанные с ними конфликты. В результате проект не урегулирует вопрос, а лишь создает впечатление, будто он урегулирован.

Декларативное упоминание риск-ориентированного подхода без его нормативного наполнения требует оценки с точки зрения принципа соразмерности, вытекающего из статей 18 и 55 Конституции РФ, поскольку без выделения категорий риска невозможно установить справедливый баланс между развитием технологий, защитой прав граждан и необходимыми ограничениями.

Негативные последствия:

- **Рост числа судебных споров.** Пользователи, авторы, платформы и разработчики будут сталкиваться в судах без четкой правовой базы.
- **Непредсказуемость для бизнеса.** Компании не смогут быть уверены в правовом статусе создаваемого контента и связанных рисках.
- **Слабая защита правообладателей.** При отсутствии специальных норм авторам будет трудно защищать свои права в новой технологической среде.
- **Риск недобросовестного использования результатов.** Пользователи будут применять контент, не понимая, насколько устойчив его правовой статус.
- **Дальнейшее накопление правовой неопределенности.** Закон должен был снять часть вопросов, но в таком виде он их только закрепляет.

15. Законопроект не реализует настоящий риск-ориентированный подход, хотя декларирует его

В тексте проекта заявлен риск-ориентированный подход, но в реальности он не воплощен в работающую правовую конструкцию. Закон не делит ИИ-системы на категории риска в юридически значимой форме и не привязывает к этим категориям разные режимы допуска, запретов, обязанностей и ответственности.

Между тем принципиально важно различать:

- низкорисковые вспомогательные системы;
- системы, влияющие на доступ к услугам;
- системы, применяемые в образовании;
- системы, работающие с детьми;
- биометрические и профилирующие решения;
- системы, затрагивающие права, обязанности и жизненные обстоятельства человека;
- решения для государственных и критических контуров.

Без этого один и тот же закон начинает одинаково смотреть на принципиально разные по опасности технологии.

Негативные последствия:

- **Чрезмерные барьеры для безобидных решений.** Низкорисковые системы могут столкнуться с ненужной бюрократией.
- **Недостаточные барьеры для опасных решений.** Высокорисковые системы, наоборот, могут получить слишком мягкий режим.
- **Неработающая модель регулирования.** Когда закон не различает уровень угроз, он не может быть ни справедливым, ни эффективным.
- **Ошибки в распределении ресурсов контроля.** Внимание регулятора будет распыляться вместо концентрации на реально опасных практиках.

- **Подрыв доверия к самому принципу регулирования.** Отрасль и граждане будут воспринимать регулирование как несбалансированное и непрофессиональное.

III. ЗАКЛЮЧЕНИЕ И ТРЕБОВАНИЯ

Исходя из изложенного, мы считаем, что проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» в текущей редакции:

- не обеспечивает должной правовой определенности;
- не создает реальных и проверяемых гарантий безопасности;
- не содержит полноценных механизмов ответственности;
- не защищает граждан от непрозрачных и технократических решений;
- не вводит специальных гарантий для детей и образовательной среды;
- создает риски административной монополизации рынка;
- допускает чрезмерное подзаконное нормотворчество;
- не соответствует масштабу и чувствительности регулируемой сферы.

В связи с этим просим:

1. **Не принимать законопроект в текущей редакции.**
2. **Вернуть его на глубокую концептуальную переработку с участием независимых технических, юридических, педагогических, психологических и этических экспертов.**
3. **Закрепить ключевые правила регулирования непосредственно в федеральном законе, а не передавать их на подзаконный уровень.**
4. **Прямо установить перечень сфер, в которых ИИ не может применяться для автономного принятия решений, влияющих на судьбу человека.**
5. **Выделить сферу образования в специальный объект правовой охраны и регулирования.**
6. **Закрепить прямой запрет на применение систем ИИ для распознавания эмоций в образовательных организациях.**
7. **Ввести особый режим обработки образовательных данных несовершеннолетних, включая запрет на их коммерческое использование и на дообучение моделей.**
8. **Установить реальные, а не декларативные стандарты распределения ответственности между разработчиком, владельцем сервиса, оператором, интегратором и пользователем.**
9. **Обеспечить прозрачность, недискриминационность и ограниченность применения механизмов реестров и доверенных моделей.**
10. **Исключить правовые лазейки, позволяющие фактически отменять понятную человеку маркировку синтетического контента.**

11. Пересмотреть положения о трансграничных технологиях и “суверенных” моделях так, чтобы защита суверенитета не превращалась в технологическую самоизоляцию.

Принятие такого закона в сыром, противоречивом и чрезмерно рамочном виде может иметь долгосрочные негативные последствия для прав граждан, для детей, для образования, для науки, для конкуренции, для технологического развития страны и для качества государственного управления.

Искусственный интеллект требует не декларативного, а точного, ответственного, профессионального и человекоцентричного регулирования. В нынешнем виде представленный законопроект этим требованиям не соответствует.