

# Российский законопроект об ИИ: в чем его опасность для прав человека?



# Оглавление

1. Введение.....	3
2. Общая характеристика и структура закона.....	3
3. Сфера действия и исключения.....	4
4. Терминология.....	5
5. Общие принципы регулирования.....	6
6. Суверенные, национальные и доверенные модели ИИ.....	7
7. Субъекты отношений и их правовой статус.....	9
8. Специфические права человека.....	11
9. Ответственность субъектов.....	12
10. Маркировка синтетического контента.....	13
11. Интеллектуальная собственность.....	14
12. Государственные органы.....	15
13. Международное сотрудничество.....	16
14. Вычислительная инфраструктура.....	17
15. Выводы.....	17

# 1. Введение

Технологии искусственного интеллекта (ИИ) стремительно трансформируют экономику и государственное управление, а также активно применяются в правоохранительной деятельности и вооружениях. В связи с этим у многих стран стоит противоречивая задача с одной стороны защитить отечественных разработчиков от экспансии внешних технологических гигантов, а с другой – экспортировать собственные технологии и регуляторные подходы. Россия долгое время воздерживалась от комплексного нормативного правового регулирования в данной сфере, занимая выжидательную позицию и отдавая предпочтение секторальному регулированию и механизмам мягкого права.

18 марта 2026 года для общественного обсуждения стал [доступен](#) проект ФЗ «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации».

Эксперты [RKS Global](#), осуществляющие систематический мониторинг развития регулирования в сфере ИИ в странах Евразии (см. доклад [«Человек против модели: как государства используют ИИ для цензуры и слежки»](#)), подготовили обзор законопроекта с акцентом на его последствия для прав человека и индустрии цифровых технологий.

## 2. Общая характеристика и структура закона

Законопроект содержит двадцать одну статью и охватывает широкий спектр вопросов: от терминологии до обязанностей отдельных субъектов, компетенции государственных органов и международного сотрудничества. При этом сам текст документа весьма неоднороден: отдельные положения описываются поверхностно, в то время как другие излишне детализированы. Например, статья 20 подробно регулирует энергетические льготы для центров обработки данных (включая преимущественное

технологическое присоединение к электросетям, льготные тарифы и освобождение от платы за присоединение), что уже частично выходит за рамки определённого в законе предмета регулирования.

Очень важный и тревожный с точки зрения фундаментальных прав человека симптом – более двадцати ключевых вопросов делегированы подзаконным актам Правительства, ФСТЭК, ФСБ и иных уполномоченных органов. Помимо этого за отдельными органами власти закрепляются новые полномочия. Например, Президент РФ теперь эксклюзивно уполномочен определять особенности применения систем ИИ в сфере обороны, национальной безопасности, общественной безопасности и правопорядка.

С точки зрения логики и юридической техники документ пока недостаточно проработан и противоречив: в тексте вводятся термины, которые не поясняются в терминологии или встречаются всего один раз, отдельные концептуальные положения включаются в текст, но не раскрываются, права и обязанности субъектов конфликтуют в рамках жизненного цикла систем ИИ. Можно предположить, что разные части документа были написаны несколькими заинтересованными сторонами в разное время, а затем объединялись в достаточно оперативные сроки. Мотиваторами такой спешки могут являться как грядущие выборы в Государственную Думу, так и наметившееся отставание в регуляторике от стран Евразийского экономического сообщества.

## **3. Сфера действия и исключения**

Часть 4 статьи 1 прямо исключает из сферы действия закона применение ИИ для целей *обороны, безопасности государства, охраны правопорядка и антитеррористической защищённости, предотвращения чрезвычайных ситуаций природного и техногенного характера*. Если исключение сферы обороны, к сожалению, является достаточно распространённым трендом для законодателей по всему миру, то исключение сферы безопасности и правопорядка является крайне тревожным сигналом. Ещё в 2023 году ЕСПЧ по делу *Glukhin*

*v. Russia* (no. 11519/20, 4 July 2023) указал на вакуум правового регулирования и фактический произвол в отношении применения технологий распознавания лиц в общественных местах со стороны органов власти. С тех пор данный вакуум так и не был регуляторно заполнен, а федеральные и региональные власти развернули значительно большее число автоматизированных систем контроля как в физическом, так и цифровом пространстве.

В части 3 также содержится информация о том, что закон будет направлен на *физических и юридических лиц*, осуществляющих деятельность в области разработки, применения, внедрения технологий искусственного интеллекта на территории РФ. Однако далее в законе раскрываются блоки, определяющие полномочия органов власти и принципы международного сотрудничества.

Предполагается, что закон, если будет принят, вступит в силу с 1 сентября 2027 года.

## 4. Терминология

Определение ИИ (п. 1 ст. 3) воспроизводит формулировку, использованную в Национальной стратегии развития ИИ 2019 года. Оно основано на критерии «имитации когнитивных функций человека», что существенно отличается от подходов, принятых на международном уровне и в большинстве юрисдикций.

Привязка к «имитации когнитивных функций человека» не даёт ясности определению и создаёт риск отсекающей части технологических решений, которые не основаны прямо на методах машинного обучения и архитектуре нейронных сетей.

Чтобы избежать этого, также введён термин «технологии ИИ», который определяет перечень технологических решений: *технологии, основанные на использовании ИИ, включающие в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы ИИ*. Однако закрепление перечня технологий на уровне закона не является оптимальным решением, именно поэтому в большинстве своём законодатели по

всему миру стараются делать текст технологически нейтральным, дополняя его за счёт рекомендаций, технических стандартов, кодексов практик и иных фреймворков.

Помимо этого в тексте закреплены определения моделей ИИ и больших фундаментальных моделей ИИ. Что касается последних, то в тексте Национальной стратегии минимальный порог для отнесения к ним составлял 1 млрд параметров (примерно уровень GPT-2 1.5B или современные маленькие модели). В текущем тексте указано, что данный порог будет в дальнейшем определён Правительством РФ. Важно отметить, что практического значения данное разграничение не имеет, так как текст в дальнейшем никак не дифференцирует требования к разработчикам обычных моделей ИИ и больших фундаментальных моделей.

## **5. Общие принципы регулирования**

В качестве одного из принципов регулирования определён риск-ориентированный подход, вероятно, как дань международным трендам и подходу ЕС, однако далее по тексту законопроекта данная концепция никаким образом не развивается: в тексте отсутствует как запрет каких-либо практик, так и разделение систем на группы в зависимости от тех рисков, которые представляет их разработка и применение.

Принцип технологической независимости предполагает разработку «суверенных и национальных моделей ИИ». Вместе с тем разработка и внедрение технологий ИИ должны осуществляться на основе традиционных российских духовно-нравственных ценностей:

*«жизнь, достоинство, права и свободы человека, патриотизм, гражданственность, служение Отечеству и ответственность за его судьбу, высокие нравственные идеалы, крепкая семья, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм,*

*взаимопомощь и взаимоуважение, историческая память и преемственность поколений, единство народов России».*

*Для контроля реализации данных положений Правительство РФ «определяет уполномоченный орган (экспертную организацию) по формированию критериев соответствия моделей, систем, сервисов искусственного интеллекта традиционным российским духовно-нравственным ценностям, а также определяет порядок его деятельности».*

Данные требования не представляется возможным в дальнейшем транслировать в конкретные метрики и технические стандарты, что фактически позволяет органам произвольно применять данные нормы и наделяет их неограниченным инструментом по контролю отношения участников рынка. Более того, такие требования создают риски по превращению моделей ИИ из нейтральных источников информации в каналы по трансляции государственной идеологии. Вкупе с продвинутыми возможностями современных моделей по убеждению людей такие системы ИИ потенциально могут превратиться в специализированный инструмент пропаганды и воздействия на общественное мнение.

## **6. Суверенные, национальные и доверенные модели ИИ**

Статья 7 раскрывает понятия «суверенных и национальных» больших фундаментальных моделей ИИ. Важно отметить, что в тексте оба понятия не раскрываются отдельно, а используются только в общем контексте.

Для того, чтобы модель была признана «суверенной и национальной», должны быть соблюдены три условия:

- 1. все стадии разработки и обучения моделей ИИ осуществляются на территории РФ;*

*2. все стадии разработки, обучения и эксплуатации моделей ИИ осуществляются гражданами РФ и российскими юридическими лицами;*

*3. обучение моделей ИИ с использованием наборов данных, формирование которых осуществляется на территории РФ гражданами РФ и российскими юридическими лицами.*

Однако конкретные критерии соответствия указанным требованиям также отнесены к дальнейшему правотворчеству Правительства РФ.

Примечательно, что в законе почти не оговариваются и позитивные последствия признания модели «суверенной и национальной». В статье 7 содержится лишь абстрактная формулировка про обеспечение благоприятных условий для разработки, внедрения и применения.

Статья 8 определяет требования к «доверенным моделям ИИ», которые эксклюзивно могут быть использованы в ГИС и объектах КИИ:

- 1. наличие подтверждения соответствия требованиям по безопасности ФСТЭК и ФСБ;*
- 2. обеспечение обработки данных исключительно на территории РФ;*
- 3. наличие подтверждения соответствия требованиям качества, установленным иными органами и госкорпорациями.*

Модели, соответствующие требованиям, включаются в специальный реестр «доверенных моделей». Порядок ведения реестра и требования к подтверждениям соответствия также определяются Правительством РФ.

Таким образом, данные положения могут быть использованы органами власти в качестве рычага давления на бизнес, если признание модели «суверенной и национальной» или «доверенной» станет важным барьером для её эксплуатации и получения финансирования. Вместе с тем расплывчатые формулировки позволят создавать упрощённый режим для крупных аффилированных с государством компаний-разработчиков систем и моделей ИИ.

# 7. Субъекты отношений и их правовой статус

Законопроект выделяет ряд субъектов и корреспондирующих им прав и обязанностей, тем самым пытаясь отразить сложность взаимодействия внутри цепочек поставок систем и моделей ИИ.

Субъект	Обязательства
<b>Разработчик модели</b> Тип продукта: Модель ИИ	Исключить предвзятости; Уведомить о запрещённых сценариях использования; Документировать архитектуру и ограничения модели; Провести моделирование рисков и определить порядок обслуживания
<b>Оператор системы</b> Тип продукта: Система ИИ	Подготовить руководство по безопасной эксплуатации (включая запрет манипуляции и эксплуатации уязвимостей); Тестировать систему на противоправные сценарии использования; Информировать пользователей о назначении и ограничениях; Обеспечивать обслуживание, незамедлительно приостанавливать эксплуатацию при угрозе вреда; Вести учёт инцидентов и назначить ответственных за обеспечение безопасности лиц
<b>Владелец сервиса</b> Тип продукта: Сервис ИИ	Установить правила доступа с запретом противоправного использования;

---

Принимать меры против злоупотреблений;

Информировать пользователей о взаимодействии с ИИ (кроме очевидных случаев);

При аудитории свыше 500 тыс. пользователей в сутки – выполнять требования для ОРИ

---

**Пользователь**

Соблюдать правила доступа к сервису;

Использовать ИИ в законных целях и не обходить встроенные механизмы безопасности

---

Несмотря на желание отразить многоступенчатость цепочек поставок «модель – система – сервис – пользователь», данные обязательства не сформулированы исчерпывающим образом. Например, разработчик модели должен только моделировать риски, однако нет речи о типологии и источниках данных рисков и требованиях по управлению ими. Также в данной статье мы видим, по сути, единственную запрещённую практику, которая более нигде не фигурирует и распространяется только на операторов систем ИИ: *«недопустимость использования системы для манипуляции поведением и эксплуатации уязвимостей человека»*. Также часть 1 статьи 10 вводит нового субъекта – *разработчика системы ИИ*, – который нигде в тексте более не встречается и отсутствует в терминологическом аппарате.

С точки зрения прав человека опасение вызывает норма, возлагающая на владельцев сервиса ИИ, к которому в течение суток обращается более 500 тыс. пользователей, находящихся на территории РФ, обязанности организатора распространения информации (ОРИ) по смыслу статьи 10.1 ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Это означает обязанность хранить на территории РФ данные о взаимодействии пользователей с сервисом, включая содержание их сообщений, и обеспечивать их доступность

для уполномоченных органов в рамках механизма, предполагающего круглосуточный удалённый доступ уполномоченного подразделения ФСБ к информационной системе ОРИ. Это также потенциально открывает широкие возможности по внедрению систем, которые позволят автоматизировать выявление нежелательного контента во взаимодействии пользователей с системами ИИ.

## **8. Специфические права человека**

Статья 9 законопроекта призвана ввести новые права граждан при использовании технологий ИИ:

1. быть информированными о применении систем ИИ при продаже товаров/услуг и об автономном принятии решений, затрагивающих их права;
2. отказаться от взаимодействия с системами ИИ (в случаях, определяемых Правительством);
3. на досудебное обжалование решений госорганов и организаций с госучастием, принятых с использованием систем ИИ;
4. на компенсацию вреда от неправомерного использования систем ИИ (в порядке, установленном ГК РФ).

Вместе с тем данные права сформулированы декларативно, по сути повторяют положения общего законодательства и не обеспечивают эффективных механизмов защиты прав человека. Нормы об информировании об автономном принятии решений сформулированы таким образом, что их возможно трактовать в крайне узком смысле: простое предоставление информации без объяснения логики принятия того или иного решения, которое затронуло права человека. Возможности по отказу от взаимодействия с системами ИИ ограничены только теми случаями, которые будут позже определены Правительством. Можно предположить, что речь будет идти только про жизненно

необходимые сервисы и услуги. Право на компенсацию вреда предусмотрено только от неправомерного использования систем ИИ в порядке, предусмотренном ГК РФ. Однако фактически новое право не создается, а даётся лишь ссылка на нормы общего права. Также не предусматривается право на компенсацию вреда, причиненного в результате функционирования продукта ненадлежащего качества при правомерном использовании системы ИИ. Также интерес вызывает и само название статьи, которая фактически распространяет данные права только на граждан РФ, игнорируя при этом иностранцев и лиц без гражданства.

## 9. Ответственность субъектов

Статья 11 законопроекта декларирует распределение ответственности между разными субъектами внутри цепочек поставок соразмерно степени вины каждого, однако никак не конкретизирует это, ссылаясь лишь на требования общего законодательства.

Также статья фактически снимает ответственность с разработчиков моделей, операторов систем и владельцев сервисов, так как она наступает только в том случае, если они *заведомо знали или должны были знать о возможности получения противоправного результата с использованием их продуктов, если иное не будет доказано в результате следственных действий*. При этом важно отметить, что статья не разграничивает разные основания наступления юридической ответственности. Можно было бы предположить, что авторы имели в виду только уголовно- и административно-правовую ответственность, так как к гражданско-правовой оговорка о следственных действиях неприменима. Однако часть 7 статьи определяет, что уголовно- и административно-правовая ответственность наступает в порядке, определённом общим законодательством.

Более того, данные субъекты также могут избежать ответственности, *если предприняли исчерпывающие меры к предотвращению*

*получения такого результата и соблюдали требования законодательства РФ.*

В совокупности данные положения создают нормативную базу, на основе которой открываются широкие возможности для произвольного правоприменения. В отдельных случаях лояльные государству компании смогут уходить от ответственности, а в других случаях возможны ограничения и показательные наказания.

Также законопроект предусматривает возможность подачи регрессных исков операторами систем в отношении разработчиков моделей в том случае, если оператор докажет, что *«вред возник исключительно вследствие недостатков объекта, которые существовали на момент его передачи оператору и не могли быть выявлены при проявлении им всей разумной осмотрительности, предусмотренной условиями эксплуатации и технической документацией»*. С одной стороны, данное положение игнорирует возникновение подобного права у ещё одного субъекта – владельца сервиса, а с другой – возлагает непропорциональное бремя доказывания на оператора системы, у которого фактически не будет способов подтвердить свою позицию при использовании закрытых (проприетарных) моделей. В свою очередь дополнительные процессуальные гарантии по раскрытию информации для нижестоящих субъектов в цепочке поставок отсутствуют.

## **10. Маркировка синтетического контента**

Все обязанности по явной и неявной маркировке синтетического контента возложены на финальное звено внутри цепочек поставок – владельца сервиса. Вместе с тем международные подходы, наоборот, исходят из необходимости вводить многоуровневую маркировку, которая будет касаться как уровня систем, так и моделей ИИ.

Следующие несколько положений были имплементированы из «Временных мер по управлению системами глубокого синтеза» КНР

(2022): возложение обязанности по проверке маркировки на держателей цифровых платформ, а также возможность исключения маркировки из сгенерированного контента при условии заключения договора с пользователем. Однако данная мера, хотя и менее обременительна для бизнеса, в меньшей степени обеспечивает прозрачность, чем в КНР, где помимо договора необходимо сохранять логи не менее шести месяцев.

## 11. Интеллектуальная собственность

Законопроект исходит из того, что сгенерированный контент не является охраноспособным по умолчанию, за исключением случаев, если он представляет собой *«исключительно оригинальные творения, соответствующие критериям охраноспособности, установленным гражданским законодательством»*. Вместе с тем данные положения напрямую противоречат логике остальных частей статьи 13, в которых передача прав на результаты интеллектуальной деятельности переложена на соглашения между разработчиком модели, владельцем сервиса и пользователем. Противоречие заключается в том, что статья, с одной стороны, не признаёт охраноспособность синтетического контента, а с другой – обязывает субъектов договариваться о распределении прав на результаты, которые могут вовсе не являться результатами интеллектуальной деятельности.

Также данная статья исходит из логики соотношения прав и обязанностей разных субъектов внутри цепочек поставок. Однако, как и в других положениях, присутствует дисбаланс: с одной стороны, разработчики моделей должны обеспечить, чтобы модели были созданы с использованием материалов, не нарушающих интеллектуальные права третьих лиц, а с другой – договор между владельцем сервиса и пользователем должен включать *«информацию о законности происхождения материала, используемого для обучения системы»*. Поставщик сервиса в большинстве случаев может не быть одновременно разработчиком

модели или оператором системы и не обладать необходимой информацией о составе наборов данных, использованных для создания модели. При этом соответствующие требования по раскрытию информации о наборах данных в законопроекте отсутствуют.

## 12. Государственные органы

Помимо отношений пользователей и коммерческих субъектов законопроект также наделяет властными полномочиями разнообразные федеральные и региональные органы.

Президент РФ будет утверждать Национальную стратегию развития ИИ (что он ранее и делал), а также определять *«особенности применения технологий ИИ в области обороны, обеспечения национальной безопасности, обеспечения общественной безопасности и правопорядка»*. Данные положения представляют опасность для прав человека, так как фактически выводят сферы общественной безопасности и правопорядка из-под исключительной компетенции законодательных органов власти. Теперь для применения систем ИИ в указанных сферах может не потребоваться принятия какого-либо закона. В перспективе данное положение приобретает особую опасность в контексте стремительного развития технологий, применяемых в сфере общественной безопасности и правопорядка: полицейской робототехники, систем предиктивного контроля, технологий распознавания речи и эмоций в местах массового скопления людей, анализа поведения через нателные камеры сотрудников правоохранительных органов, автоматизированного мониторинга социальных сетей. Каждая из этих технологий несёт значительные риски для права на неприкосновенность частной жизни, свободы собраний, свободы выражения мнений и запрета дискриминации.

Основные полномочия по осуществлению правотворческих и управленческих функций закреплены за Правительством РФ и

отдельным компетентным органом, который будет определён в дальнейшем. Сейчас эти функции исполняет Минцифры.

Отдельные полномочия закреплены и за органами власти субъектов РФ, однако, учитывая узкие предметы их ведения, определённые Конституцией РФ, можно предположить, что по большей части их деятельность будет направлена на межрегиональное сотрудничество и реализацию федеральной политики. С точки зрения нормативных правовых актов стоит ожидать прямое копирование федеральных законов в данной сфере.

## **13. Международное сотрудничество**

Статьи 15–18 определяют векторы международного сотрудничества в сфере ИИ и носят преимущественно программно-декларативный характер. В целом акцент сделан на «лидирующую роль» России, формирование «единого пространства доверенных технологий ИИ», продвижение российских подходов и стандартов.

Статья 17 касается так называемых «трансграничных технологий ИИ». В ней закреплены положения, создающие правовую основу для дальнейшего ограничения или запрета использования иностранных технологий ИИ на территории РФ: функционирование трансграничных технологий искусственного интеллекта может быть запрещено или ограничено в случаях, установленных законодательством РФ.

Расплывчатость формулировок в сочетании со статьей 7 (суверенные и национальные модели) формирует контуры для режима цифрового изоляционизма в сфере ИИ по аналогии с остальной сферой Интернета и цифровых технологий. В дальнейшем это может привести к запрету использования таких популярных сервисов и моделей, как ChatGPT, Claude, Llama, Mistral и т.д. В свою очередь это сильно отразится на российском бизнесе, который в значительной мере использует иностранные системы и модели для создания своих продуктов. Таким образом, бизнес будет

вынужден либо обходить ограничения, чтобы продолжать пользоваться иностранными сервисами через VPN или задействовать иностранные компании-прокладки, либо использовать китайские аналоги. Компании, которые рассчитывают на участие в государственных проектах или закупках, будут вынуждены использовать только ПО российских производителей.

## 14. Вычислительная инфраструктура

Статья 20 детально регулирует создание и эксплуатацию центров обработки данных (суперкомпьютеров) для целей ИИ, включая конкретные экономические льготы: преимущественное подключение к электросетям, освобождение от платы за подключение, сниженные тарифы на электроэнергию, налоговые льготы, бюджетное финансирование.

Уровень детализации этих положений плохо сочетается с остальным текстом документа. Эти нормы скорее относятся к отдельному отраслевому акту или программе государственной поддержки. Их включение в закон об ИИ создаёт впечатление наличия лоббистского интереса определённой отраслевой группы.

## 15. Выводы

1. Законопроект декларирует риск-ориентированный подход, но фактически его никак не реализует: отсутствует классификация систем по уровням риска, не определены запрещённые практики, не установлены дифференцированные обязательства. Фактическим стержнем регулирования является не управление рисками, а контроль допуска – через реестр доверенных моделей и режим суверенных и национальных моделей.
2. Сфера обороны, национальной и общественной безопасности, правопорядка выведена из-под действия закона и передана

в исключительную компетенцию Президента РФ. Это означает, что применение систем ИИ именно в тех областях, где риски для прав человека наиболее высоки – распознавание лиц, предиктивная полиция, автоматизированный контроль – остаётся в нормативном вакууме, на который указал ЕСПЧ ещё в 2023 году.

3. Введение духовно-нравственных ценностей в качестве критерия оценки моделей ИИ не имеет аналогов в мировой практике. Данные требования не являются транслируемыми в технические стандарты и бизнес-процессы и в совокупности с размытыми критериями допуска в реестр создают механизм сегментации рынка, в котором доступ определяется не качеством модели, а лояльностью разработчика.
4. Права граждан сформулированы декларативно и не обеспечены механизмами, которые были бы эффективны для защиты прав. Право на информирование сведено к уведомлению о факте применения систем ИИ без раскрытия логики принятия решений. Право на отказ от взаимодействия с системами ИИ обусловлено решением Правительства и, вероятнее всего, будет ограничено узким перечнем случаев. Компенсация вреда привязана к «неправомерности» использования и отсылает к общим нормам ГК РФ.
5. Режим ответственности выстроен в пользу разработчиков и операторов: формулировка «заведомо знали или должны были знать» в сочетании с возможностью освобождения при соблюдении «исчерпывающих мер» создаёт условия для избирательного правоприменения. Информационная асимметрия внутри цепочек поставок не компенсируется процессуальными гарантиями по раскрытию информации.
6. Более двадцати ключевых вопросов отнесены к компетенции Правительства, ФСТЭК, ФСБ и иных органов, что размывает роль федерального закона в системе нормативного правового регулирования. Для субъектов это означает невозможность оценить свои обязательства до принятия подзаконных актов. Также это открывает широкие возможности по произвольному толкованию положений закона правоприменителями, что создает угрозу нарушений прав человека.

7. Связка статей 7, 8 и 17 формирует трёхуровневый режим ограничения внутреннего рынка: преференции для отечественных разработчиков (суверенные и национальные модели), допуск через государственную сертификацию (реестр доверенных моделей) и правовая основа для запрета иностранных технологий (трансграничные ограничения). В совокупности с декларативным характером статей о международном сотрудничестве это указывает на то, что законопроект ориентирован не на интеграцию в глобальную регуляторную среду, а на формирование замкнутого национального контура в сфере ИИ, впрочем как и всего контура суверенного интернета.
8. В совокупности законопроект в его текущей редакции представляет собой не столько инструмент защиты прав граждан и управления рисками ИИ, сколько нормативную инфраструктуру для государственного контроля над рынком ИИ и его участниками.