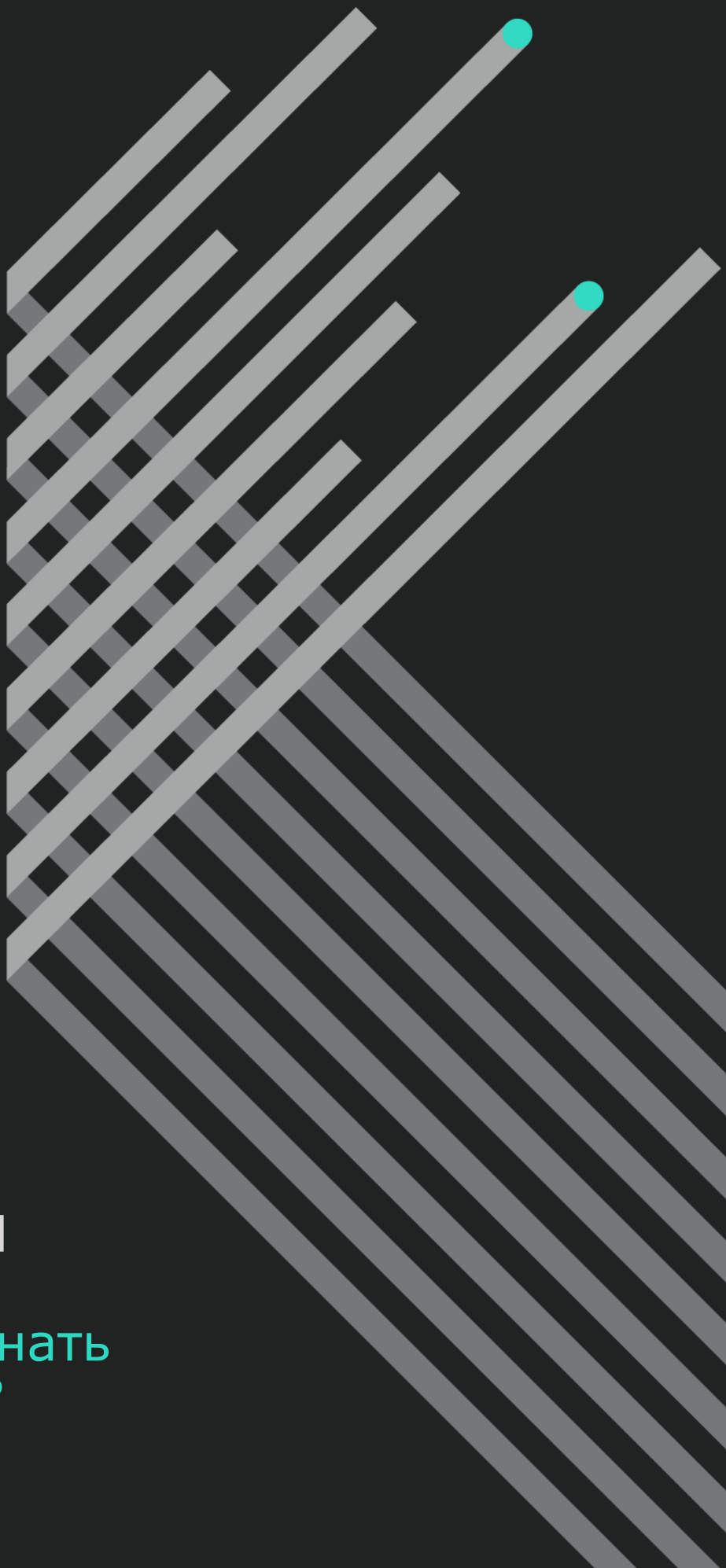
BGP LITIGATION

комплексная
правовая
поддержка

bgplaw.com



Закон об ИИ в России: что нужно знать уже сейчас?

18 марта 2026 г. опубликован законопроект «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» (далее - Законопроект). Документ охватывает полный цикл разработки, внедрения и применения ИИ-систем на территории России. При этом он содержит ряд специфических требований, учитывающих отечественный регуляторный контекст.

Законопроект выступает первым актом, регулирующим не отдельные вопросы применения искусственного интеллекта в конкретных случаях, а устанавливающим то самое глобальное «мягкое» регулирование.

В отличие от Регламента Европейского Союза «Об установлении единых правил в области искусственного интеллекта», Законопроект сосредоточился на ключевых зонах регулирования, распределив более точечные вопросы между другими органами государственной власти.

В Законопроект заложены серьезные основы, определяющие вектор дальнейшего развития отечественного рынка ИИ и подходов к его использованию. Отдельное внимание уделено ключевым вопросам: принципы, безопасность, ответственность.

На кого распространяется?

Законопроект распространяется на физических и юридических лиц, осуществляющих деятельность в области разработки, применения и внедрения технологий ИИ на территории Российской Федерации. Вводится пятизвенная система субъектов:

- разработчик модели искусственного интеллекта;
- оператор системы искусственного интеллекта;
- владелец сервиса искусственного интеллекта;
- пользователь сервиса искусственного интеллекта;
- органы государственной власти в пределах их полномочий.

Такое разграничение отражает логику цепочки ответственности: каждый субъект несет обязательства соразмерно своей возможности влиять на результат работы ИИ-системы.

Закон по общему правилу не применяется к отношениям, возникающим в связи с применением ИИ-технологий в целях обороны и безопасности государства.

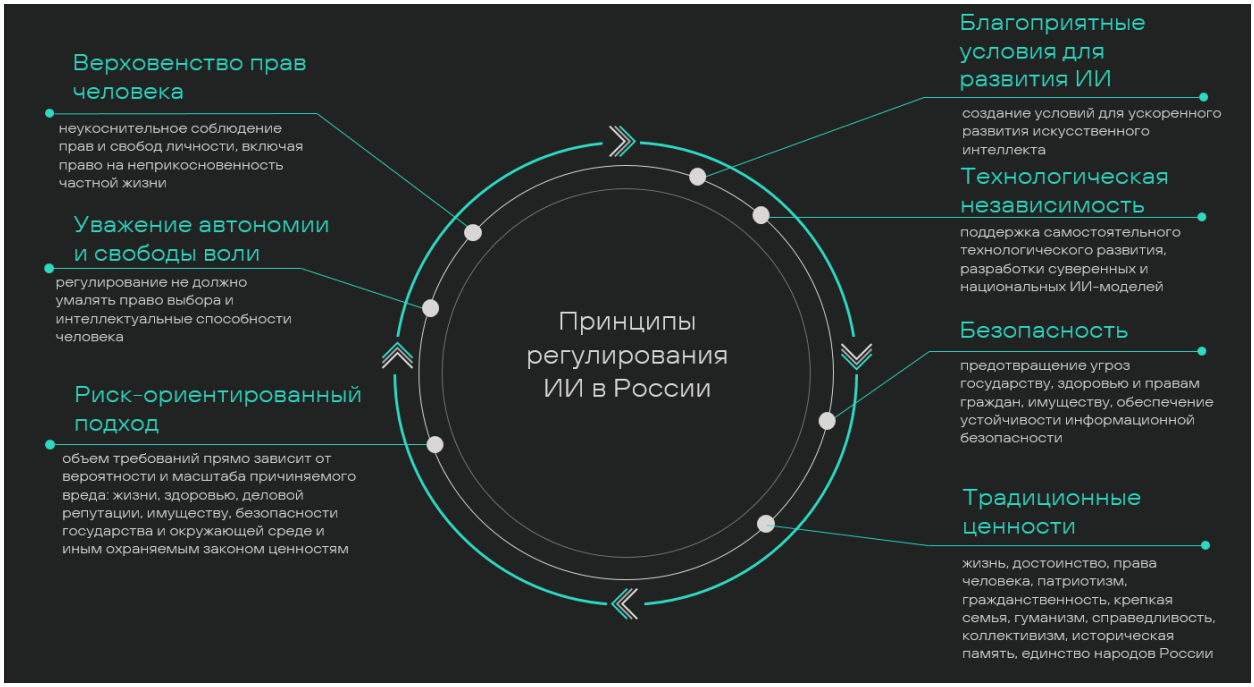
Принципы регулирования

Законопроект закрепляет семь базовых принципов регулирования сферы ИИ. В основе - верховенство прав и свобод человека, включая защиту персональных данных и неприкосновенность частной жизни, а также уважение автономии и свободы воли: регулирование не должно ограничивать интеллектуальные способности и право выбора гражданина.

Центральным инструментом является риск-ориентированный подход - объем требований к субъекту определяется вероятностью и масштабом потенциального вреда. Параллельно закреплен принцип технологической независимости,

предполагающий приоритетную поддержку суверенных и национальных ИИ-моделей. Принцип безопасности направлен на предотвращение угроз конституционному строю, жизни и здоровью граждан, имуществу и интересам государства.

Отдельно выделен принцип учета традиционных российских духовно-нравственных ценностей при разработке и применении ИИ-технологий. Наконец, законопроект декларирует создание благоприятных условий для развития отрасли, тем самым обозначая, что регулирование задумано не как ограничительное, а как рамочное.



Риск-ориентированный подход соотносится с логикой Регламента Европейского Союза «Об установлении единых правил в области искусственного интеллекта»: это «мягкое» регулирование, наиболее логичное для быстро меняющейся технологической среды. При оценке конкретной ИИ-системы учитываются назначение, вероятность и масштаб риска, степень автономности, влияние на юридически значимые решения и категория обрабатываемой информации (закрытая/публичная).

Суверенные и национальные модели

Закон вводит понятие суверенных и национальных больших фундаментальных моделей (БФМ). Разделение между суверенной и национальной моделью в текущей версии отсутствует, для обеих моделей предъявлен одинаковый набор требований:

- **территориальная разработка и обучение**: все стадии осуществляются исключительно на территории РФ;
- **субъектный состав**: все стадии разработки, обучения и эксплуатации - только гражданами РФ и российскими юридическими лицами;
- **данные для обучения**: формирование наборов данных осуществляется на территории РФ гражданами РФ и российскими юридическими лицами.

Реестр доверенных моделей

К применению в государственных информационных системах (ГИС) и на значимых объектах критической информационной инфраструктуры (КИИ), принадлежащих госорганам и госкорпорациям, допускаются только доверенные модели ИИ из соответствующего реестра. Для признания модели доверенной необходимо выполнение трех условий одновременно:

- **соответствие требованиям безопасности**, установленным ФСТЭК и ФСБ;
- **обработка данных исключительно на территории РФ** при применении модели ИИ;
- **соответствие отраслевым требованиям качества**, установленным профильными ФОИВ, государственными корпорациями или Банком России применительно к соответствующей отрасли.

Единого универсального стандарта качества нет.Требования будут отличаться в зависимости от отрасли. Пока не ясно, как именно будет проходить подтверждение качества моделей, если они одновременно будут использоваться в различных отраслях и как в целом будет выглядеть порядок подтверждения – ответы на эти вопросы должно дать Правительство РФ.

Разделение обязанностей субъектов

Вместе с созданием структуры субъектов авторы законопроекта предлагают разделение обязанностей в зависимости от их степени влияния на функциональные возможности искусственного интеллекта.

Разработчик обязан:

- исключить из модели функциональные особенности, способные привести к дискриминации по поведению или личностным характеристикам;
- информировать оператора (в оригинальном опубликованном тексте на момент подготовки алерта указано «разработчика») системы ИИ о невозможности ее использования в запрещенных целях;
- документировать архитектуру, логику функционирования и ограничения модели в объеме, достаточном для проверки соответствия законодательству;
- проводить моделирование потенциальных рисков применительно к предполагаемому использованию;
- определить порядок обслуживания и контроля параметров функционирования.

Оператор обязан:

- включить в документацию руководство по безопасной эксплуатации с прямым запретом на использование системы для манипуляции поведением и эксплуатации уязвимостей человека;
- проводить тестирование системы на предмет возможности ее использования в противоправных целях;

- предоставлять пользователям информацию о функциональном назначении и ограничениях системы;
- обеспечить техническое обслуживание и контроль параметров функционирования объектов с использованием искусственного интеллекта;
- незамедлительно приостанавливать эксплуатацию при выявлении угрозы причинения вреда жизни, здоровью граждан, безопасности государства, имуществу или окружающей среде;
- вести учет инцидентов, связанных с функционированием объектов ИИ;
- назначить ответственных лиц за безопасное функционирование.

Владелец сервиса обязан:

- определить правила доступа к сервису с прямым запретом на использование в противоправных целях;
- принимать меры по недопущению противоправного использования сервиса;
- информировать пользователей о взаимодействии с ИИ-системой (за исключением очевидных случаев);
- при суточной аудитории свыше 500 000 пользователей с территории РФ - выполнять обязанности, предусмотренные ст. 10.1 Федерального закона № 149-ФЗ;
- определить порядок обслуживания и контроля объектов с ИИ;
- внедрить механизмы, ограничивающие генерацию контента, противоречащего законодательству РФ.

Пользователь обязан:

- соблюдать установленные правила доступа к сервису;
- использовать сервис и модели ИИ в целях, не противоречащих законодательству;
- не совершать действий, направленных на обход встроенных механизмов безопасности и контроля в нарушение установленных параметров функционирования объектов с использованием ИИ.

Норма о запрете обхода механизмов безопасности прямо охватывает случаи взлома и несанкционированного изменения поведения ИИ-системы. Граница между допустимым использованием и «обходом» в тексте законопроекта не раскрыта, но очевидно, что такие методики как data poisoning, prompt injection скорее попадают под этот запрет. Это одна из самых интересных частей законопроекта, поскольку его авторы затрагивают реальные прикладные ситуации использования ИИ, зная сценарии пользовательского поведения и фактические методы противоправной работы с нейросетями.

Права граждан при использовании технологий ИИ

Законопроект формирует комплекс прав граждан, ранее не закрепленных в российском законодательстве. Все они являются продолжением общего вектора

законодательства на защиту граждан и важны для бизнеса, который активно внедряет ИИ в свои процессы.

- **Право на раскрытие информации об ИИ**. Лицо, осуществляющее продажу товаров или оказание услуг с использованием ИИ без участия человека в принятии решений, обязано проинформировать об этом потребителя.
- **Право на объяснение решения**. При принятии автономных решений, затрагивающих права и законные интересы гражданина, он вправе потребовать разъяснения принятого решения и его пересмотра с участием человека.
- **Право на получение услуги без участия ИИ**. В случаях, устанавливаемых Правительством РФ, организации, оказывающие услуги с применением ИИ, обязаны обеспечить альтернативный «ручной» канал обслуживания.
- **Право на досудебное обжалование**. Гражданин вправе оспорить решения органов государственной власти и иных субъектов, принятые с использованием ИИ.
- **Право на компенсацию вреда**. Гражданин имеет право на возмещение вреда, причиненного неправомерным использованием технологий ИИ, в порядке, установленном гражданским законодательством РФ.

Норма об альтернативном сервисном канале имеет серьезные операционные последствия: сегодня ИИ глубоко встраивается в клиентское обслуживание в банкинге, телекоме, e-commerce. Компаниям, чьи бизнес-процессы полностью выстроены вокруг ИИ, потребуется заблаговременно разработать резервный операционный контур.

Это, само собой, несет достаточно большие операционные издержки – большинство компаний, внедривших ИИ, уже оптимизировали свои расходы на «физическое» обслуживание. Несмотря на то, что законопроект вступает в силу только в сентябре 2027 г., этого времени может не хватить для полной оптимизации процессов с учетом новых требований, поэтому бизнесу рекомендуется приступить к реинжинирингу в ближайшее время.

Идентификация синтезированного контента

Законопроект вводит отдельный режим работы с аудио- и видеоматериалами, сгенерированными с помощью ИИ. Такой режим поможет защитить граждан от дипфейков, качество и рост числа которых стремительно увеличивается с каждым днем.

- **Обязательная маркировка**. Владелец сервиса ИИ обязан размещать информационное предупреждение в составе синтезированного материала в формате, воспринимаемом и человеком, и машиной (своего рода техническая маркировка). При этом такая маркировка должна быть в том же виде, что и сам материал – аудио или видео.
- **Ответственность соцсетей**. Владельцы соцсетей (лица, указанные в части 1 статьи 10.6 Федерального закона «Об информации, информационных технологиях и о защите информации») при достижении 100 000 пользователей в сутки обязаны самостоятельно проверять контент на предмет его

синтетического происхождения, удалять немаркированный контент или предупреждать пользователей об отсутствии маркировки.

- **Отказ от маркировки по соглашению сторон**. Стороны вправе договором предусмотреть отсутствие информационного предупреждения; такой отказ должен быть предметным, информированным и добровольным.
- **Удаление маркировки - правонарушение**. Лица, осуществляющие обработку синтезированного материала с целью удаления информационного предупреждения, несут административную ответственность по законодательству РФ – какую именно законопроект не раскрывает.
- **Права третьих лиц**. Пользователи сервисов ИИ обязаны соблюдать права и интересы третьих лиц при использовании синтезированного контента.

Дополнительные обязанности для владельцев соцсетей по работе с ИИ-контентом – одно из самых важных изменений. Как и в случае с бизнесом, использующим ИИ, техническая подготовка к автоматизированному выявлению синтезированного материала требует больших ресурсов и времени.

Персональные данные

ИИ неразрывно связан с персональными данными (далее – ПДн). В первую очередь потому, что обучение моделей основано на их обработке на всех этапах жизненного цикла – от сбора до эксплуатации. Связь ИИ и ПДн прослеживается в Законопроекте, но раскрывается пока лишь декларативно. На уровне принципов закрепляется приоритет защиты частной жизни и ПДн, вводится требование об учете категории обрабатываемой информации (общедоступная информация, информация ограниченного доступа или иная), провозглашается риск-ориентированный подход.

В Законопроекте указано, что данные необходимы для разработки и развития моделей ИИ. Однако при этом ответа на вопрос - как именно должна обеспечиваться правомерность обработки данных для этой цели, т.е. какое правовое основание из ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – 152-ФЗ) необходимо выбрать (e.g. базовое согласие, или актуальный нынче законный интерес) - в Законопроекте нет.

Второй проблемный аспект – это соблюдение принципа целевой обработки (ч. 2 ст. 5 152-ФЗ). Для обучения ИИ это требование трудно соблюсти, так как наборы данных могут переиспользоваться, комбинироваться и применяться для совершенно иных целей, которые не были известны на этапе сбора. Поэтому без введения специального режима или исключений для исследовательских целей развитие ИИ может оказаться в серой зоне.

В Законопроекте также предпринимается попытка закрыть риски, которые возникают при использовании ИИ – профилирование, дискриминация, отсутствие прозрачности. Так, вводятся требования об уведомлении субъектов о применении ИИ, о маркировке ИИ-контента. Но при этом уровень защиты в части принятия автоматизированных решений в проекте заметно ниже, чем в 152-ФЗ.

По общему правилу запрещено принятие решений, которые порождают юридические последствия для субъекта или влияют на его права и законные интересы, на основании исключительно автоматизированной обработки персональных данных (ст. 16 152-ФЗ). Исключение – письменное согласие субъекта, которое практически невозможно получить в случае с использованием ИИ. В проекте закона (ст. 9) речь идет только об уведомлении субъекта о принятии любых решений ИИ, а также о праве субъектов обжаловать такие решения. Но процедурных гарантий, например, в части требований к объяснимости принятого ИИ решения или качеству данных, не появляется.

Интеллектуальная собственность

Один из самых обсуждаемых вопросов использования ИИ – права на объекты ИС, сгенерированные нейросетями. Законопроект решает этот вопрос, внося ясность в дискуссии сообщества о режиме охраны таких объектов.

- **Режим охраны.** Объекты интеллектуальной собственности, созданные с применением ИИ-сервисов, охраняются в порядке, предусмотренном ГК РФ. При этом объектами интеллектуальной деятельности признаются только оригинальные творения, соответствующие критериям охраноспособности, - независимо от степени участия ИИ.
- **Обязанности владельца сервиса.** Уведомлять пользователей о правилах и ограничениях использования результатов ИД до начала работы с сервисом; обеспечивать доступ, использование и выгрузку созданных материалов строго в соответствии с договором; включать в пользовательское соглашение условие о принадлежности прав на сгенерированный контент.
- **Ограничения для пользователей.** Запрещается использовать результаты, полученные через ИИ-сервис, способами, нарушающими нормы об авторском праве и смежных правах, а также способом, противоречащим условиям договора с владельцем сервиса.
- **Обязанности разработчиков.** Обеспечить возможность доступа и выгрузки РИД, созданных с помощью их модели; при разработке гарантировать отсутствие нарушений прав на РИД.
- **Text and data mining**. Прямо закреплено, что извлечение информации из охраняемых объектов в рамках компьютерного анализа текстов и данных не является нарушением авторских или патентных прав.

Вычислительная инфраструктура: центры обработки данных

Важной частью законопроекта выступили нормы, устанавливающие преференции для развития центров обработки данных (ЦОД) – авторы явно осознают необходимость обеспечения технической мощности для реализации тех принципов, которые заложены в законопроект. Так, Правительство РФ вправе утвердить перечень ЦОД, необходимых для развития ИИ. Включение в перечень влечет существенный пакет льгот и преференций:

- приоритетное и частично безвозмездное технологическое присоединение к сетям, упрощенный порядок согласования схем электропотребления, приоритетный доступ к электроэнергии от государственных генерирующих объектов;

- право приобретать электроэнергию по регулируемым сниженным тарифам и заключать долгосрочные договоры с закреплением предельного уровня цены;
- бюджетное финансирование, налоговые льготы и льготы по аренде государственного имущества;
- инфраструктурная поддержка, включая предоставление объектов недвижимости и оборудования.

Требования к ЦОД, включаемым в перечень, устанавливает Правительство РФ. С учетом требований о сверхмощной инфраструктуре для высоконагруженных сервисов содержание подобных объектов доступно крайне ограниченному числу игроков рынка. Однако указанные нормы должны стимулировать развитие данной отрасли, что позволит продолжить вектор на хранение всех данных в отечественном технологическом контуре.

Ответственность

Законопроект вводит принцип «цепочечной» ответственности: каждый субъект отвечает за тот этап жизненного цикла ИИ-системы, на котором он мог влиять на результат.

Субъект	За что отвечает
Разработчик Оператор Владелец сервиса	Несут ответственность за вред, причиненный вследствие недостатков разработанных и используемых моделей и систем - если такие недостатки могли быть выявлены ими при проявлении разумной осмотрительности. Исключения – если они предпринимали меры к предотвращению получения вредоносного результата работы
Пользователь	Несет ответственность за использование результата работы с ИИ, нарушающего закон, если такой результат получен умышленно или в случае несоблюдения пользователем условий использования ИИ

Особые исключения для операторов и пользователей: не несут ответственности в случае наличия непреодолимой силы, умысла потерпевшего, скрытых недостатков ИИ и противоправных действий третьих лиц, которые они не могли предотвратить.

Право регресса оператора к разработчику: оператор, возместивший вред, вправе предъявить регрессное требование к разработчику, если будут доказаны недостатки ИИ, возникшие по вине разработчика.

Уголовная и административная ответственность за нарушение законодательства в сфере применения ИИ наступает в порядке, установленном законодательством РФ. Конкретные санкции в тексте законопроекта не раскрыты – ожидается, что они будут установлены позднее.

> *Механизм атрибуции вреда по цепочке субъектов с высокой долей вероятности потребует разработки методологии, которая позволит технически локализовать момент негативного влияния на модель. На текущем этапе практика по подобным спорам в России отсутствует и ее развитие будет требовать обязательного вовлечения экспертов, обладающих узкой экспертизой в разработке и функционировании искусственного интеллекта*

Государственный контроль и мониторинг

Обеспечение безопасного использования, согласно законопроекту, будет возложено на государство в формате мониторинга и своевременного реагирования. За это будут отвечать уполномоченные ФОИВ, которые отвечают за:

- сбор и систематизацию информации об инцидентах, угрозах и рисках информационной безопасности;
- оценку масштаба и характера негативных последствий инцидентов;
- прогнозирование возникновения угроз и рисков.

При выявлении угрозы, способной причинить существенный вред правам граждан или интересам государства, **ФОИВ вправе инициировать внеплановую проверку** оператора системы ИИ, а также **выдавать обязательные предписания об устранении нарушений.**

Выводы и перспективы

Законопроект выступает первой ступенью перехода от декларативного к содержательному регулированию: закреплены конкретные обязанности участников рынка, права граждан и механизмы государственного контроля. Выбор риск-ориентированного подхода выглядит наиболее сбалансированным для технологической среды. Это принципиально важный сигнал: регулятор стремится не сдержать развитие ИИ, а упорядочить его.

Вместе с тем значительная часть ключевых параметров вынесена на нижестоящее регулирование - отраслевые требования к качеству моделей, критерии для ЦОД, порядок маркировки синтезированного контента, конкретные санкции. Это создает период регуляторной неопределенности, на который заложены следующие полтора года. Компаниям, откладывающим адаптацию до появления финальных актов, рискуют оказаться в ситуации острого дефицита времени: вступление в силу запланировано на 1 сентября 2027 г., однако подготовка инфраструктуры, документации и корпоративных процессов потребует значительных ресурсов. Компаниям, активно внедряющим ИИ, рекомендуется уже сейчас начать подготовку к изменениям и провести аудит бизнес-процессов.

Требования к локализации и разработке отечественных моделей формируют новый барьер входа на рынок разработки ИИ. В условиях, когда суверенные и национальные модели получат государственную поддержку и преференциаль-

ный доступ к инфраструктуре, конкурентные позиции иностранных разработчиков будут существенно слабее. Рынок, по всей видимости, будет консолидироваться вокруг нескольких крупных игроков, способных соответствовать всей совокупности требований.

Стоит отметить и то, что тренд риск-ориентированных подходов, который ранее задавал только ЕС, становится глобальным стандартом.И отечественный законопроект, несмотря на собственную специфику, движется в том же направлении. Это означает, что компании, выстроившие комплаенс-процессы с ориентацией на международные практики, скорее всего окажутся лучше подготовлены к любым итоговым изменениям текста. Уже сейчас целесообразно определить внутренние регламенты работы с ИИ, зафиксировать их в корпоративных политиках и пользовательских соглашениях.

Как подготовиться к изменениям?

- провести аудит процессов, в которых используется ИИ;
- разработать собственную политику использования ИИ;
- если ИИ используется в работе с клиентами - подготовить альтернативные способы оказания услуг без участия ИИ;
- если компания работает в госсекторе – подготовиться к использованию отечетственных ИИ-сервисов.

Дополнительно

Более подробно погрузиться в вопросы ожидаемых изменений и провести операционную и техническую подготовку к нововведениям может помочь практика Legal Tech и автоматизация процессов BGP Litigation

BGP LITIGATION

комплексная правовая поддержка

ДЦ «Империя», Пресненская наб., д. 6, стр. 2
г. Москва, Россия 123112

+7 (495) 777 28 20 office@bgplaw.com bgplaw.com

Евгений Журба

Партнер
Legal Tech и автоматизация процессов

evgeniy.zhurba@bgplaw.com

Арсений Топадзе

Советник, адвокат
Защита данных и цифровое регулирование

arseniy.topadze@bgplaw.com

Никита Соколов

Юрист
Legal Tech и автоматизация процессов

nikita.sokolov@bgplaw.com

Мария Константинова

Младший юрист
Защита данных и цифровое регулирование

mariia.konstantinova@bgplaw.com