

Требования к программному обеспечению и моделям искусственного интеллекта, применяемым на объектах КИИ и ЗОКИИ

9 апреля 2026 г.

С 1 марта 2026 года вступил в силу Федеральный закон от 31.07.2025 № 325-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее — **«Закон»**), который вносит системные изменения в порядок допуска программного обеспечения к использованию на объектах критической информационной инфраструктуры Российской Федерации (далее — **«КИИ»**) и в государственных информационных системах (далее — **«ГИС»**).

Одновременно 18 марта 2026 года для общественного обсуждения опубликован проект Федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации»¹ (далее — **«Законопроект об ИИ»**), планируемое вступление в силу которого — 1 сентября 2027 года.

Оба нормативных акта продолжают государственное регулирование в сфере использования программного обеспечения на объектах КИИ для обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации. Требования к допуску программного обеспечения для использования на объектах КИИ и значимых объектах КИИ (далее — **«ЗОКИИ»**) последовательно устанавливаются в пользу специального — «доверенного» — программного обеспечения, программно-аппаратных комплексов и технологий ИИ. Таким образом, формируется единая система контроля над ИТ-инфраструктурой критически важных объектов.

Настоящий обзор систематизирует требования указанных нормативных актов к программному обеспечению и моделям искусственного интеллекта, применяемым на объектах КИИ и ЗОКИИ.

1. Выводы

1.1 Требования к программному обеспечению (действуют с 1 марта 2026 года)

- (i) С 1 марта 2026 года для использования на объектах КИИ вводится дополнительный Реестр ПО для собственных нужд, равнозначный Единому реестру российского ПО. Программное обеспечение на объектах КИИ должно быть включено в один из указанных реестров — это минимальное обязательное условие правомерного использования.
- (ii) Для ЗОКИИ требования усилены: при проведении закупок наивысший приоритет получает ПО, включённое в Реестр доверенного ПО.

¹ Проект Федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации» // Федеральный портал проектов нормативных правовых актов, ID 166424, [опубликован](#) 18.03.2026.

- (iii) Закупки иностранного ПО для использования на ЗОКИИ требуют согласования с уполномоченным федеральным органом исполнительной власти.
- (iv) Субъекты КИИ, эксплуатирующие ЗОКИИ, обязаны завершить переход на доверенные программно-аппаратные комплексы к 1 января 2030 года.

1.2 Требования к моделям искусственного интеллекта по Законопроекту об ИИ²

- (i) К применению в ГИС и на ЗОКИИ, принадлежащих государственным органам, учреждениям и предприятиям, допускаются исключительно доверенные модели ИИ, включенные в Реестр доверенных моделей.
- (ii) Применительно к объектам КИИ, не относящимся к государственным, Законопроект не предусматривает прямого требования об обязательном использовании доверенных моделей ИИ. Вместе с тем Правительство РФ наделяется полномочием устанавливать такое требование для отдельных объектов КИИ и ЗОКИИ по предложению отраслевых федеральных органов исполнительной власти, что не исключает возможность расширения обязательных требований.
- (iii) Трансграничные модели ИИ, обрабатывающие данные за пределами Российской Федерации, не соответствуют критерию территориальности и не смогут быть включены в Реестр доверенных моделей. Функционирование трансграничных технологий искусственного интеллекта может быть запрещено или ограничено в случаях, установленных законодательством Российской Федерации.
- (iv) Законопроект квалифицирует модель ИИ как разновидность программы для ЭВМ, однако не разрешает вопрос о необходимости её одновременного включения в соответствующие реестры ПО, что требует мониторинга изменения Законопроекта или принятия подзаконных актов.

2. Три новых реестра программного обеспечения

С 1 марта 2026 в России введены три новых специализированных реестра, дополняющих действующий Единый реестр российского ПО³:

- **Реестр ПО для собственных нужд:** предназначен для ПО, разработанного для внутреннего использования компаний, позволяя при этом применять его на объектах КИИ без включения в Единый реестр российского ПО.
- **Реестр доверенного ПО:** предназначен для российского ПО с повышенным уровнем доверия, которое соответствует более строгим требованиям безопасности. Для включения в реестр ПО уже должно находиться в Едином реестре российского ПО или в Реестре для собственных нужд. Статус «доверенного» является конкурентным преимуществом, особенно при закупках для ЗОКИИ.
- **Реестр значимых разработчиков:** предназначен для ключевых ИТ-компаний, находящихся под контролем РФ, её субъектов или граждан и заключивших с Правительством соглашение о разработке или модернизации ПО за счёт собственных средств в целях импортозамещения в рамках особо значимых проектов.

² Приведенные выводы основаны на тексте Законопроекта об ИИ, находящегося на стадии общественного обсуждения. Окончательные требования могут быть скорректированы, рекомендуется мониторинг изменений.

³ Единый реестр российских программ для электронных вычислительных машин и баз данных.

Ведение реестров возложено на Минцифры России⁴. Правила формирования и ведения устанавливаются Правительством РФ.

В развитие положений Закона Правительством РФ приняты ключевые подзаконные акты, конкретизирующие порядок ведения каждого из реестров:

- Постановление Правительства РФ от 28.11.2025 № 1931⁵ — устанавливает правила формирования и ведения перечня доверенного ПО;
- Постановление Правительства РФ от 28.11.2025 № 1936⁶ — устанавливает правила формирования и ведения перечня ПО для собственных нужд;
- Постановление Правительства РФ от 28.11.2025 № 1937⁷ — вносит изменения в ПП № 1236 в отношении Единого реестра российского ПО в связи с введением новых реестров.

3. Требования к ПО на объектах КИИ

В соответствии с Законом, Федеральным законом от 07.04.2025 № 58-ФЗ⁸ и принятыми подзаконными актами, **ПО, используемое на объектах КИИ должно быть включено в Единый реестр российского ПО или в Реестр ПО для собственных нужд**. Оба варианта являются равнозначными для целей выполнения требования об использовании российского ПО на объектах КИИ. На данном уровне статус «доверенного ПО» не является обязательным условием допуска для использования ПО на объектах КИИ, однако предоставляет конкурентное преимущество при закупках.

Ключевые критерии для включения в реестр ПО для собственных нужд:

- **Принадлежность исключительных прав.** Исключительное право на ПО должно принадлежать Российской Федерации, её субъекту, муниципальному образованию, российской некоммерческой организации, неподконтрольной иностранным лицам, российской коммерческой организации, находящейся под контролем Российской Федерации, её субъекта, муниципального образования или гражданина РФ, либо гражданину РФ. Под контролем понимается возможность определять решения, принимаемые указанной российской коммерческой организацией, в силу наличия права прямо или косвенно распоряжаться более чем 50% общего количества голосов, приходящихся на голосующие акции (доли), составляющие уставный капитал данной российской коммерческой организации.
- **Отсутствие сведений, составляющих государственную тайну.** Сведения о ПО не должны составлять государственную тайну, и ПО не должно содержать таких сведений.

⁴ Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

⁵ Постановление Правительства РФ от 28.11.2025 № 1931 «Об утверждении Правил формирования и ведения перечня доверенных российских программ для электронных вычислительных машин и баз данных».

⁶ Постановление Правительства РФ от 28.11.2025 № 1936 «О перечне российских программ для электронных вычислительных машин и баз данных, разработанных и используемых для собственных нужд российскими юридическими лицами».

⁷ Постановление Правительства РФ от 28.11.2025 № 1937 «О внесении изменений в некоторые акты Правительства Российской Федерации» (в части корректировки Постановления Правительства РФ от 16.11.2015 № 1236).

⁸ Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ».

Основанием для включения ПО в перечень является решение президиума Правительственной комиссии, принимаемое по результатам рассмотрения заявления правообладателя. Для успешного прохождения процедуры необходимо одновременное соблюдение строгого комплекса требований, основными из которых являются безусловная принадлежность исключительных прав российским субъектам и использование ПО исключительно для внутренних нужд. Критически важные критерии включают:

- **Суверенитет прав:** Исключительное право на ПО на территории всего мира и на весь срок действия исключительного права должно принадлежать российским лицам, как указано выше.
- **Технологическая независимость:** Полный запрет на выплаты иностранным лицам за права и услуги, связанные с разработкой и модификацией ПО. Вся инфраструктура хранения исходного кода, компиляции, активации и управления лицензиями должна располагаться и контролироваться на территории России.
- **Внутреннее использование:** ПО должно использоваться правообладателем исключительно для собственных целей или предоставляться связанным российским организациям.
- **Совместимость ПО:** Обязательным условием является совместимость хотя бы с одной операционной системой из реестра российского ПО или ЕАЭС, а также отсутствие в этом реестре ПО со сходным функционалом.

4. Требования к ПО на значимых объектах КИИ (ЗОКИИ)

Для ЗОКИИ установлены усиленные требования, включающие все требования, предусмотренные для объектов КИИ, а также дополнительные:

- **Приоритет доверенного ПО при закупках.** При проведении закупок для ЗОКИИ наивысший приоритет получает ПО, включённое в Реестр доверенного ПО. ПО, не имеющее статуса «доверенного», получает сниженный приоритет. Таким образом, при наличии доверенной альтернативы участник без соответствующего статуса де-факто проигрывает тендер.
- **Переход на преимущественное использование российского ПО.** Заказчики, осуществляющие закупки по Федеральному закону от 18.07.2011 № 223-ФЗ, не вправе осуществлять закупки иностранного ПО для использования на принадлежащих им ЗОКИИ без согласования с уполномоченным ФОИВ⁹. Требования к ПО, используемому на ЗОКИИ, а также правила перехода на преимущественное использование российского ПО установлены Постановлением Правительства РФ от 22.08.2022 № 1478¹⁰.
- **Переход на доверенные программно-аппаратные комплексы (ДПАК).** Указом Президента РФ от 30.03.2022 № 166 Правительству РФ поручено определить сроки и порядок перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им ЗОКИИ. Во исполнение

⁹ Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

¹⁰ Постановление Правительства РФ от 22.08.2022 № 1478 «Об утверждении требований к программному обеспечению, используемому на значимых объектах критической информационной инфраструктуры Российской Федерации, и Правил согласования закупок иностранного программного обеспечения».

данного поручения Постановлением Правительства РФ от 14.11.2023 № 1912¹¹ установлены правила такого перехода.

Для квалификации в качестве доверенного, ПАК должен удовлетворять следующим критериям: сведения о ПАК должны быть включены в единый реестр российской радиоэлектронной продукции; ПО в составе комплекса соответствует требованиям к программам для ЗОКИИ; при наличии функции защиты информации — имеется документ ФСТЭК и (или) ФСБ России.

Переход должен быть завершён к 1 января 2030 года.

Критерии включения в Реестр доверенного ПО: для получения статуса доверенного ПО необходимо одновременное соблюдение общих и специальных требований для конкретных классов ПО (системное ПО, офисное ПО, средства обеспечения информационной безопасности, промышленное ПО).

Ключевые общие требования:

- **Суверенитет прав:** программное обеспечение должно быть предварительно зарегистрировано в одном из установленных государственных реестров (российского ПО или ПО для собственных нужд), а его разработка и модификация должны осуществляться силами правообладателя или с привлечением исключительно российских исполнителей.
- **Контроль обновлений:** критически важным условием является полный контроль над процессами обновления, которые не только требуют согласия пользователя, но и должны выполняться исключительно с использованием инфраструктуры на территории России, без доступа к зарубежным серверам.
- **Технологическая независимость:** правообладатель обязан иметь всю необходимую инфраструктуру для разработки, сборки и тестирования ПО в изолированном окружении на территории РФ, включая полный доступ к исходным кодам и средствам разработки из отечественного реестра. Установлен полный запрет на выплаты иностранным лицам за права и услуги, связанные с разработкой и модификацией ПО.
- **Безопасность:** обязательства по безопасности включают создание службы технической поддержки по всей стране, ведение автоматизированного учёта уязвимостей и их обязательное устранение в течение 30 дней с момента публикации в банке данных угроз безопасности информации ФСТЭК России, а для ПО со средствами защиты информации — наличие соответствующего сертификата.
- **Экспертиза:** для включения в реестр необходимо пройти экспертизу в аттестованном центре тестирования, который подтвердит соответствие ПО установленным требованиям.

5. Законопроект об ИИ: требования к моделям искусственного интеллекта на объектах КИИ и ЗОКИИ

Законопроект об ИИ впервые на законодательном уровне закрепляет правовую рамку для разработки, внедрения и использования технологий искусственного интеллекта в Российской Федерации. Документ вводит понятийный аппарат (система ИИ, сервис ИИ, модель ИИ, большая фундаментальная модель и т.д.), устанавливает права и обязанности участников рынка и закрепляет риск-ориентированный подход: требования к системам ИИ

¹¹ Постановление Правительства РФ от 14.11.2023 № 1912 «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».

определяются в зависимости от назначения технологии, уровня автономности, характера обрабатываемых данных и возможного вреда.

Законопроект вводит следующие категории моделей ИИ:

- **Суверенная модель ИИ** — модель, все стадии разработки, обучения и эксплуатации которой осуществляются на территории РФ гражданами России и российскими юридическими лицами, с использованием наборов данных, сформированных на территории РФ, без использования компонентов, разработанных за пределами страны.
- **Национальная модель ИИ** — модель, аналогичная суверенной, но с допустимым ограниченным использованием иностранных наборов данных (конкретные критерии будут установлены подзаконными актами).
- **Доверенная модель ИИ** — модель, включённая в специальный Реестр доверенных моделей искусственного интеллекта и допущенная к использованию в ГИС и на ЗОКИИ. В реестр доверенных моделей могут также включаться суверенные и национальные модели.

Применительно к объектам КИИ Законопроект об ИИ не предусматривает прямого требования об обязательном использовании доверенных моделей для всех субъектов КИИ.

К применению в государственных информационных системах и на ЗОКИИ, принадлежащих государственным органам, государственным учреждениям и государственным предприятиям, допускаются исключительно доверенные модели ИИ, включённые в соответствующий реестр.

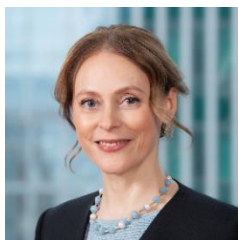
Отмечаем, что Законопроект наделяет Правительство РФ полномочием устанавливать случаи обязательного применения доверенных моделей на отдельных объектах КИИ или ЗОКИИ по предложению отраслевых ФОИВ, что оставляет возможность расширения требования на любые объекты.

Критерии включения в Реестр доверенных моделей ИИ:

- **Безопасность:** подтверждение соответствия требованиям безопасности, установленным ФСТЭК России и ФСБ России. Подтверждение включает проверку на наличие уязвимостей, недеklarированных возможностей и устойчивость к внешним воздействиям.
- **Территориальность:** обеспечение обработки данных исключительно на территории Российской Федерации.
- **Качество:** подтверждение соответствия требованиям, устанавливаемым профильными федеральными органами исполнительной власти, государственными корпорациями или Банком России в соответствующих отраслях.

* * *

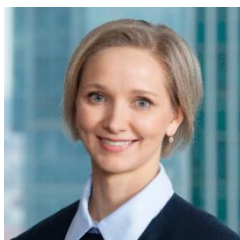
Мы будем рады ответить на ваши вопросы по данной тематике.



Анна Максименко

Партнер

Anna.Maximenko@kkmp.legal



Елена Полевая

Старший юрист

Elena.Polevaya@kkmp.legal