

Регуляторная аналитика

Информационные технологии

Тренды регулирования IT-индустрии в 2026 году



Оглавление

Ключевые особенности регуляторной политики в IT-индустрии за 2026 год.....	3
1. Усиление и детализация регулирования критической информационной инфраструктуры.....	4
2. Переход к системному обеспечению киберустойчивости	7
3. Пересмотр подходов к регулированию интеллектуальной собственности.....	10
4. Формирование регуляторной рамки для искусственного интеллекта	13
5. Регулирование платформенной экономики.....	16
6. Цифровой и технологический суверенитет	19
7. Переход к более адресной модели государственной поддержки.....	21
Авторы.....	27

Ключевые особенности регуляторной политики в IT-индустрии за 2026 год

В 2026 году государственное регулирование IT-индустрии продолжило развиваться одновременно по нескольким направлениям. В уже сформировавшихся и чувствительных сферах регулирования, прежде всего в области критической информационной инфраструктуры (КИИ) и кибербезопасности, акцент смещается в сторону детализации требований, усиления контроля и повышения ответственности бизнеса. Одновременно государство формирует и донастраивает регуляторные рамки для новых и быстро развивающихся сегментов цифровой экономики, включая искусственный интеллект (ИИ) и платформенную экономику.

Отдельной особенностью регуляторной политики становится дальнейшее закрепление цифрового и технологического суверенитета в качестве сквозного приоритета. Поддержка отечественных решений, требования к происхождению и безопасности ПО, импортозамещение и снижение зависимости от зарубежных технологий все в большей степени интегрируются в регулирование отдельных сфер IT-индустрии.

Таким образом, регуляторную политику и логику принимаемых государственных решений нельзя назвать однородными. В них прослеживаются следующие ключевые направления:

- Развитие и детализация регулирования чувствительных областей (КИИ, кибербезопасность и др.);
- Формирование регуляторных рамок для новых и перспективных отраслей (ИИ, платформенная экономика);
- Политика по поддержке отечественных решений и выстраиванию цифрового суверенитета (национальные цифровые платформы, решения в области софта и др.).

Данные направления не являются исчерпывающими, но формируют ключевые тренды государственного регулирования в 2026 году. Они же определяют темпы нормотворчества, приоритеты внимания регуляторов, а также позиции и роль ключевых государственных стейкхолдеров.

В рамках этих направлений среди ключевых трендов в регулировании отрасли наиболее значимыми являются следующие:

1. Регулирование критической информационной инфраструктуры;
2. Переход к системному обеспечению киберустойчивости;
3. Пересмотр подходов к регулированию интеллектуальной собственности;
4. Регулирование искусственного интеллекта;
5. Регулирование платформенной экономики;
6. Цифровой и технологический суверенитет;
7. Переход к более адресной модели государственной поддержки.

Каждый из указанных трендов характеризуется собственной логикой развития регулирования, набором регуляторных инструментов и потенциальными последствиями для участников IT-отрасли, которые рассматриваются далее.

1. Усиление и детализация регулирования критической информационной инфраструктуры

Ключевой особенностью регулирования в этом году стало ужесточение контроля за субъектами критической информационной инфраструктуры (КИИ)¹. При этом акцент сместился с разового выполнения требований регуляторов по обеспечению защищенности объектов в сторону постоянного контроля и управления безопасностью. Все это реализуется за счет регулярной актуализации сведений об объектах, оценки уровня их защиты, проверки применяемых средств и обеспечения постоянного обмена информацией с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА).

Развитие нормативной базы опирается на уже вступившие с 01.09.2025 в силу изменения в профильный Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»². В частности, уже тогда были затронуты следующие значимые направления регулирования:

- Существенно расширены полномочия Правительства РФ в части регулирования.
- Заложена нормативная основа для обеспечения системного перехода на российское ПО и программно-аппаратные комплексы (ПАК) на значимых объектах КИИ.
- Доработана система показателей критериев значимости объектов КИИ.
- Предусмотрено формирование перечней типовых объектов КИИ.
- Заложены основы для расширения механизмов отраслевого регулирования процесса категорирования объектов.

В этом году последовательно реализовывалось расширение и углубление данной рамки.

1. Единый перечень типовых отраслевых объектов КИИ

В феврале 2026 года был утвержден единый перечень типовых отраслевых объектов КИИ — около 400 позиций, охватывающих 14 ключевых отраслей: здравоохранение, науку, транспорт, связь, энергетику, банковский и финансовый сектор, оборонную промышленность и др.³

2. Отраслевые особенности категорирования объектов КИИ

В 2026 году отраслевые министерства опубликовали особенности категорирования объектов КИИ в области связи⁴, атомной энергетики⁵, банковской и иных сферах финансового рынка⁶, научной сферы⁷ и ряде других отраслей.

3. Риск-ориентированный подход к регулированию

С 01.03.2026 вступили в силу разработанные ФСТЭК России изменения⁸, которые переводят защиту объектов КИИ на риск-ориентированную модель:

- Вводится коэффициент защищенности информации (КЗИ), рассчитываемый по 16 критериям (не реже 1 раза в 6 месяцев).
- Предусматривается также показатель уровня зрелости процессов защиты информации (ПЗИ) — рассчитывается не реже 1 раза в 2 года.

- Непрерывный мониторинг и жесткие сроки устранения уязвимостей (критические — до 24 часов, высокие — до 7 календарных дней).
- Расширение круга регулируемых лиц — включая не только владельцев государственных информационных систем (ГИС), но и организации, взаимодействующие с ними (подрядчиков, интеграторов).

4. Перевод объектов КИИ на отечественные решения

В мае 2026 года сообщалось о предложении Минцифры России установить дифференцированные предельные сроки перехода на отечественное ПО — до 01.01.2028 в общих случаях, а также до 01.01.2031 и 01.01.2036 в ряде исключений. На данный момент изменения не были утверждены.

При этом отсутствует единая точка зрения на требования к доверенному софту, у которого будет приоритет в госзакупках. В сентябре сообщалось, что на данный момент бизнес ориентируется в первую очередь не на ПО, а на компанию — разработчика. В версии Минцифры России сделан акцент на проверке продукта и списка критериев для каждого типа софта.

5. Ужесточение ответственности за нарушения в сфере КИИ

В апреле 2026 года Президент РФ подписал законы о поправках в Уголовный кодекс РФ⁹ и в КоАП РФ¹⁰, которые не только ужесточили ответственность за нарушения, но и установили уголовную ответственность за «уничтожение, блокирование, модификацию и копирование компьютерной информации, содержащейся в КИИ».

В июне 2026 года Минцифры России сообщало о планах подготовить законопроект о введении «серьезных» штрафов для компаний за несоблюдение сроков перевода значимых объектов КИИ на российское ПО. Законопроект на данный момент не был опубликован.

Ключевые выводы:

- Законодательство в сфере КИИ в 2026 году проходит трансформацию к системному, риск-ориентированному подходу. В рамках него большую роль играет не только наличие необходимых мер защиты, но и способность организаций своевременно выявлять угрозы,

реагировать на инциденты и поддерживать работу критических систем.

- Импортозамещение и переход на российское ПО все теснее связываются с защитой объектов КИИ и обеспечением условий их работы. При этом параллельно прорабатываются сроки данного перехода, а также ужесточается ответственность за несоблюдение требований регуляторов.

Прогноз:

1. Рост роли требований к доверенному софту

В значительной степени траекторию развития рынка КИИ определяют требования, предъявляемые к доверенному софту.

При этом ключевыми факторами станут репутация компании-разработчика, а также сертификация продукта. От деталей устанавливаемых критериев будет зависеть возможность снижения барьеров для сохранения доступа к рынку со стороны небольших разработчиков.

2. Значимость роли дифференцированных сроков перехода на отечественное ПО

Планируемая дифференциация сроков перехода на отечественное ПО призвана обеспечить бесперебойное функционирование отраслей на протяжении переходного периода.

В этих условиях у бизнеса сохраняется возможность лоббирования условий и критериев перехода на отечественные решения с учетом общих интересов регуляторов и отрасли.

2. Переход к системному обеспечению киберустойчивости

В 2026 году регулирование сферы кибербезопасности развивается под воздействием сразу нескольких факторов: роста числа кибератак, усиления требований к КИИ, дальнейшей локализации IT-ландшафта и ужесточения требований к защите ГИС и данных. Одновременно повышается ответственность организаций за самостоятельное обеспечение устойчивости и реагирование на угрозы.

1. Изменение порядка взаимодействия субъектов

С 30.01.2026 действует приказ ФСБ России, устанавливающий обновленный порядок обмена информацией о компьютерных атаках и инцидентах¹¹. Он предусматривает следующее:

- Установление обмена информацией не только о компьютерных инцидентах, но и об атаках.
- Информация об атаках и инцидентах, полученная при обмене с другими субъектами КИИ, будет направляться в Национальный координационный центр по компьютерным инцидентам (НКЦКИ).
- Устанавливаются жестко регламентированные сроки информирования НКЦКИ об инцидентах и атаках на объекты КИИ.

2. Правила и технические условия для работы со средствами защиты от кибератак

С 10.01.2026 действуют положения приказа ФСБ России, которые касаются правил и технических условий для работы со средствами защиты от кибератак на объекты КИИ — в части обнаружения, предупреждения, ликвидации и др.¹² Приказ также включает определение порядка их установки, подключения к ресурсам и обеспечения непрерывной работы.

3. Рост автономности решений бизнеса

В апреле 2026 года ФСТЭК России утвердила методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах»¹³.

Документ актуализирует и систематизирует мероприятия и процессы защиты информации. Акцент делается на понимании угроз, управлении рисками и контроле за борьбой с ними. Помимо «формальной проверки» наличия средств защиты акцент смещается на понимание угроз, управление рисками и контроль борьбы с ними.

4. Усиление требований к защите ГИС

С 01.09.2026 вступили в силу требования приказа ФСТЭК России в части обеспечения безопасности объектов ГИС¹⁴. Среди них — новые требования к нормам безопасности, техническим мерам защиты и порядку работы с информацией, обрабатываемой в ГИС.

Также с 01.09.2026 вступили в силу положения приказа ФСТЭК России об изменении порядка аттестации на соответствие требованиям по защите информации ограниченного доступа¹⁵.

Ключевые выводы:

- Заметным трендом является переход от отдельных средств защиты к регулированию способности организации обеспечивать постоянную киберустойчивость.
- Усиливается государственный контур реагирования на кибератаки через развитие ГосСОПКА, а также детализацию регулирования.
- Средства реагирования бизнеса и процессы взаимодействия с регуляторами выступают в качестве взаимосвязанных элементов единого контура кибербезопасности.

Прогноз:

1. Рост роли требований к доверенному софту

С учетом ужесточения требований к поставщикам ПО увеличиваются риски снижения конкуренции до нескольких крупнейших игроков на рынке.

При этом перед регуляторами стоит двойная задача: с одной стороны, повышать уровень безопасности и защищенности систем за счет ужесточения требований к ним, а с другой — сохранить доступ отечественных разработчиков к соответствующему рынку.

2. Расширение ответственности бизнеса за обеспечение защищенности

Переход к модели проактивного мониторинга угроз в сфере кибербезопасности и реагирования на них способствует повышению общей зрелости рынка, а также формирует для регуляторов основу для дальнейшего повышения требований.

В перспективе это увеличивает шансы на проработку мер по ужесточению ответственности за ненадлежащее управление рисками.

3. Пересмотр подходов к регулированию интеллектуальной собственности

Регулирование вопросов интеллектуальной собственности (ИС) развивается по нескольким, отчасти разнонаправленным трекам: с одной стороны, происходит ослабление защиты правообладателей от антимонопольного вмешательства в интересах конкуренции, с другой — усиливается защита от прямых нарушений исключительных прав.

1. Проработка отмены антимонопольных иммунитетов

В 2026 году ФАС России продолжила работу над проектом поправок к закону «О защите конкуренции»¹⁶, которые предусматривают отмену антимонопольных иммунитетов для правообладателей интеллектуальной собственности (включая ПО). Впервые данную позицию озвучил глава ФАС России М. Шаскольский еще в 2024 году — по его словам, это не отразится на уровне защиты прав правообладателей, но позволит развивать конкуренцию «на цифровых и смежных с ними товарных рынках».

Действующее законодательство о защите конкуренции выводит из-под отдельных антимонопольных запретов действия правообладателей, связанные с использованием принадлежащих им результатов интеллектуальной деятельности, в том числе программного обеспечения. Иными словами, в ряде случаев правообладатели могут определять условия использования своей интеллектуальной собственности без применения к ним общих антимонопольных ограничений.

ФАС России считает, что такими иммунитетами могут злоупотреблять крупные компании, в частности устанавливая разные цены для отдельных регионов и категорий потребителей без экономического обоснования. Ведомство предлагает предоставить антимонопольному регулятору возможность вмешиваться в подобных случаях, если действия правообладателя приводят к ограничению конкуренции на товарном рынке.

В июне 2026 года отраслевые ассоциации (включая АПКИТ и РУС-СОФТ) направляли обращения профильным ведомствам с просьбой не поддерживать подготовленную версию законопроекта. Согласно аргументам отрасли, распространение антимонопольных запретов на ИС нарушает логику защиты нематериальных активов, ослабляя

позиции российских разработчиков ПО в конкуренции с уходящими западными вендорами.

В настоящее время «шестой антимонопольный пакет», посвященный, по словам представителей ФАС России, отмене иммунитетов для ИС, еще не внесен в Госдуму РФ — отрасль продолжает добиваться более мягкой редакции, учитывающей ее интересы.

2. Ужесточение ответственности за нарушение ИС

С 04.01.2026 вступили в силу поправки в Гражданский кодекс РФ, которые изменили правила определения и взыскания компенсации за нарушение исключительных прав¹⁷. Согласно изменениям:

- Уточнены правила определения размера компенсации, закреплено понятие отдельного нарушения.
- Установлены специальные правила для случаев, когда одно нарушение затрагивает сразу несколько объектов ИС. В частности, суды получили больше возможностей учитывать совокупный характер таких нарушений и снижать итоговый размер компенсации.
- Одновременно усилена ответственность за отдельные нарушения: максимальный размер компенсации увеличен с 5 до 10 млн руб.

Для бизнеса изменения имеют разнонаправленный эффект: правообладатели получили возможность требовать более высокую компенсацию, тогда как для нарушителей снижены риски несоразмерного многократного взыскания за взаимосвязанные нарушения.

3. Регулирование ИС в сфере ИИ

Нормы и положения законодательства об ИС не в полной мере отвечают на вопросы регулирования новых отраслей и сфер, связанных прежде всего с развитием ИИ.

Согласно принятому закону о регулировании ИИ¹⁸, обучение моделей не является нарушением авторских или смежных прав: допускаются извлечение и анализ данных, а также их краткосрочная запись для обучения моделей. Важным условием для использования ИС является «правомерное получение или публичный доступ к объектам ИС».

При этом отраслевые союзы (включая НП ППП) уже выступили с критикой данного положения, подчеркивая ущемление интересов авторов и противоречие нормам Гражданского кодекса РФ.

В результате отдельные аспекты использования объектов ИС при разработке и обучении моделей остаются недостаточно урегулированными. В отсутствие детализированных требований значительная часть практических подходов к использованию таких объектов формируется самими участниками рынка. Это сохраняет правовую неопределенность как для правообладателей, так и для разработчиков ИИ и создает предпосылки для дальнейшей конкретизации регулирования и формирования правоприменительной практики.

Ключевые выводы:

- Регуляторный подход к ИС продолжает трансформироваться: от ее восприятия преимущественно как объекта правовой охраны — к признанию ее потенциальным инструментом ограничения конкуренции.
- ИИ становится «зоной конфликта» между стимулированием инноваций и защитой ИС. Чем активнее модели будут обучаться на контенте, защищенном ИС, тем выше вероятность дальнейшей конкретизации правил доступа к данным и использования объектов ИС.
- Попытка регуляторов усилить контроль за использованием ИС через изменение антимонопольных иммунитетов встречает жестокое сопротивление IT-отрасли.

Прогноз:

1. Вероятна попытка выстроить дифференцированное регулирование

Полная отмена иммунитетов будет продолжать сталкиваться с сопротивлением отрасли. Более реалистичным сценарием выглядит появление исключений для отдельных антиконкурентных практик.

Наиболее чувствительными для крупных российских разработчиков могут стать вопросы ценовой политики, условий лицензирования и другие коммерческие практики, которые сегодня находятся в зоне иммунитета.

2. Ключевая роль бизнеса в стимулировании инноваций и защите ИС

В ближайшей перспективе компаниям придется учитывать одновременно несколько изменяющихся факторов — позицию ФАС России по

антимонопольным иммунитетам, ужесточение защиты ИС и регулирование ИИ.

Ключевым направлением развития дискуссии для бизнеса должно стать обеспечение предсказуемости регулирования, особенно в части защиты прав и связанных с ними рисков для нарушителей.

4. Формирование регуляторной рамки для искусственного интеллекта

В конце июля Президент РФ подписал закон о поддержке развития технологий ИИ в РФ. Его положения закладывают основу для регулирования разработки и применения ИИ с акцентом на поддержку общественных решений.

Изначально рассматриваемая версия закона носила более комплексный характер — включая общее регулирование сферы, запрет на использование иностранных моделей, требования по использованию исключительно российских данных. Однако итоговое регулирование сфокусировалось на более точечной поддержке наиболее передовых и комплексных российских моделей.

Ключевые положения закона:

- Вводится понятие «большой фундаментальной модели» — системы с не менее чем 1 млрд параметров, выполняющей интеллектуальные задачи на уровне результатов деятельности человека или выше.
- Закрепляются категории «суверенных» и «национальных» ИИ-моделей, которые должны создаваться и управляться российскими разработчиками.
- Аудио- и видеоматериалы, созданные или существенно измененные с помощью ИИ, подлежат специальной маркировке с 01.03.2027.
- Разработчикам больших фундаментальных моделей разрешено использовать для обучения материалы без согласия правообладателей при соблюдении установленных законом условий.
- Сохраняется роль государства в чувствительных сферах — Правительство РФ отдельно установит случаи исключительного использования «суверенных» и «национальных» моделей. Для доступа

таких моделей к федеральным информационным системам могут быть установлены специальные правила по согласованию с ФСБ России.

Основные положения вступили в силу с 01.09.2026, положения о полномочиях Правительства РФ начнут действовать с 01.03.2027, а для уже внедренных моделей, не соответствующих новым критериям, предусмотрен переходный период до 01.09.2032 при условии обработки данных на территории РФ.

С учетом повышенного внимания государства к отрасли для руководства и координации ее развития были сформированы отдельные органы. Указом Президента РФ была создана специальная Комиссия по вопросам развития технологий ИИ под руководством вице-премьера — руководителя Аппарата Правительства РФ Д. Григоренко и заместителя руководителя Администрации Президента РФ М. Орешкина¹⁹. Кроме того, в марте была создана Подкомиссия по развитию и внедрению искусственного интеллекта (ИИ) под руководством Д. Григоренко. В сферу ее ответственности входят решение вопросов внедрения технологий в различных отраслях, а также координация работы ведомств. В начале августа была создана Рабочая группа «Медиаиндустрия и авторское право» при Правительстве РФ, которая занялась подготовкой предложений по регулированию отрасли ИИ.

Параллельно ведется работа по доработке и уточнению законодательства, к которой привлекаются и представители бизнеса:

1. Использование экспериментальных правовых режимов (ЭПР)

В конце июня были опубликованы изменения в законодательстве в части расширения сферы ЭПР на случаи, когда правовые отношения на данный момент еще не урегулированы²⁰. Согласно поправкам, режим ЭПР может применяться в отношении сферы ИИ — механизм позволяет тестировать ИИ-решения в условиях временных изъятий из общего регулирования.

В рамках этого бизнес уже предложил Минэкономразвития России и Минцифры России создать в рамках ЭПР платформу для обучения ИИ с доступом к государственным данным, включая отраслевые ГИС, реестры и ведомственные системы.

2. Меры господдержки

Летом Минпромторг России обсуждал с компаниями-разработчиками

введение балльной системы для определения уровня локализации чипов для ИИ и ограничения позиций иностранных разработчиков.

Кроме того, рабочая группа при Совете по кодификации предлагала ввести механизм самостоятельного ограничения использования произведений для обучения ИИ через единый портал организации по коллективному управлению правами (ОКУП).

Также в сентябре Минцифры России опубликовало для общественного обсуждения проект постановления Правительства РФ о наделении ведомства полномочиями в части регулирования сферы ИИ.

3. Инициативы бизнеса

В августе 2026 года «Яндекс» представил Правительству РФ концепцию «национального датасета» — набора тестовых заданий и эталонных данных для тестирования моделей на предмет их соответствия «духовно-нравственным ценностям». При этом итоговое решение по его использованию не было принято.

В сентябре 2026 года стало известно, что в рамках Рабочей группы Подкомиссии по развитию и внедрению технологий ИИ по предложению бизнеса обсуждались льготное кредитование и лизинг для производства компонентов для отечественной ИИ-отрасли.

4. Исключительное использование отечественных ИИ-моделей

В начале сентября 2026 года на полях ВЭФ вице-премьер — руководитель Аппарата Правительства РФ Д. Григоренко сообщал о планах по исключительному использованию российского ИИ в ряде сфер, таких как безопасность, проведение выборов, госуправление и образование.

Ключевые выводы:

- Сфера ИИ является одной из зон повышенного внимания российских властей с учетом ее значимости и актуальности для современной экономики.
- С учетом комплексного характера отрасли текущий фокус регулирования направлен скорее на точечную поддержку крупных и значимых отечественных моделей, нежели на попытку охватить всю отрасль в целом.

- Сохраняется высокая роль бизнеса в проработке подзаконных актов, а также в оценке практического эффекта изменений от внедрения ИИ в различных отраслях и сферах.

Прогноз:

1. Акцент в регулировании будет смещаться в сторону управления рисками

Текущее регулирование носит скорее рамочный характер и задает общие приоритеты восприятия отрасли со стороны властей.

По мере развития технологий ИИ и расширения их применения вероятен переход от регламентации самого факта использования ИИ к регулированию сопутствующих рисков.

2. Проработка дифференцированных требований к разработке и использованию ИИ

По мере перехода от «ИИ как инструмента» к «ИИ как активному участнику бизнес-процессов» фокус регулирования будет смещаться в сторону анализа различных сценариев подобного использования.

Вероятна разработка дифференцированных требований к отраслям в зависимости от уровня риска, а также появление требований в части программных решений.

5. Регулирование платформенной экономики

С 01.10.2026 вступает в силу Федеральный закон о регулировании платформенной экономики²¹, который задает регуляторную рамку функционирования цифровых платформ в России.

Закон устанавливает требования к деятельности операторов цифровых платформ и их взаимодействию с партнерами и пользователями. Среди ключевых положений:

- Закон вводит понятия цифровой платформы, посреднической цифровой платформы, оператора, партнера, карточки товара и ПВЗ.
- Маркетплейсы обязаны проверять карточки товаров на полноту информации перед публикацией. Несоответствующие

требованиям карточки не будут допускаться к публикации или будут удаляться.

- Вводится запрет на изменение логистических или коммерческих условий «задним числом».

Вводится реестр посреднических платформ, подлежащих регулированию — согласно данным Минэкономразвития России, в реестр будут включены 12 платформ, из них 11 — это крупнейшие российские ресурсы (маркетплейсы, агрегаторы услуг, включая такси и сервисы доставки).

При этом, согласно утвержденным Правительством РФ критериям²², в реестр могут быть включены платформы, соответствующие следующим требованиям:

- Среднесуточная аудитория не менее 100 тыс. пользователей из России за предыдущий календарный год.
- Платформа должна соответствовать одному из двух показателей: не менее 10 тыс. партнеров, совершивших хотя бы одну оплаченную сделку за год, или совокупная стоимость сделок на сумму от 50 млрд руб. за год.

Платформам с иностранным владельцем для включения в реестр нужно подтвердить аудиторию 100 тыс. пользователей в сутки на территории России.

Отдельно поправками в КоАП РФ вводится ряд штрафов для владельцев платформ за каждое фиксируемое нарушение: их размер составит для юрлиц от 50 до 500 тыс. руб.²³

При этом архитектура регулирования платформ на данный момент не достигла финальной стадии.

1. Второй пакет мер и поправок

Минэкономразвития России подготовило и опубликовало для общественного обсуждения второй пакет мер по регулированию платформенной экономики, а также связанные поправки в КоАП РФ. Среди основных положений:

- Регулируются вопросы расчетов с селлерами и условий работы российских продавцов.
- Уточняются правила отказа от товара и возврата.

- Расширяются правила работы реестра цифровых платформ.
- Расширяется административная ответственность маркетплейсов.

Предполагаемая дата вступления изменений в силу — 01.03.2027.

Ранее Подкомиссия по развитию цифровых платформ Правительственной комиссии по цифровому развитию утвердила «дорожную карту» развития регулирования платформенной экономики на 2026–2027 годы.

2. Эксперимент по расширению доступа к госзакупкам

В августе 2026 года Президент РФ подписал закон о предоставлении части образовательных учреждений (школы, колледжи, детские сады) возможности проводить госзакупки на отечественных маркетплейсах «с полки», без организации тендеров²⁴. Эксперимент пройдет с 01.10.2026 до 30.09.2028.

В сентябре 2026 года стало известно, что Минэкономразвития России прорабатывает требования к маркетплейсам для эксперимента по ограниченному участию в указанных госзакупках. Такие площадки должны:

- быть включены в реестр цифровых платформ Минэкономразвития России;
- иметь логистическую инфраструктуру минимум в 45 регионах России;
- располагать предложениями как минимум двух продавцов по товарам из перечня Минпросвещения России²⁵.

Ключевые выводы:

- Формируется контур регулирования цифровых платформ: государство выделяет платформы в отдельный объект регулирования и устанавливает для них специальные правила.
- Власти стремятся сбалансировать интересы участников платформенной экономики, поскольку регулирование охватывает отношения между платформами, продавцами, исполнителями и потребителями.
- Одной из важных задач регуляторов является ограничение дисбаланса между платформами и их партнерами, а также российскими и иностранными участниками рынка.

Прогноз:

1. Проработка расширения критериев регулирования

С учетом охвата действующим регулированием всех крупных IT-платформ в России, в дальнейшем возможно расширение пороговых критериев включения в реестр.

2. Детализация требований к участникам отрасли

На данный момент регулирование платформ рассматривается как детализация отношений между продавцом и покупателем. Одним из следующих акцентов в части регулирования может стать детализация требований к самим платформам, в том числе в части технологической инфраструктуры отрасли.

6. Цифровой и технологический суверенитет

В 2026 году меры по обеспечению цифрового и технологического суверенитета перестали восприниматься как отдельная приоритетная задача регуляторов и бизнеса и вошли в контур постоянной работы. Их реализация продолжается, а соответствующие подходы регулярно дорабатываются и корректируются с учетом развития технологий и совершенствования регулирования.

1. Требования к происхождению ПО

С 01.03.2026 вступило в силу постановление Правительства РФ²⁶, которое вводит новые требования к программному обеспечению для включения в реестр российского и евразийского ПО и получения им приоритета в рамках госзакупок:

- Вводится трехуровневая система классификации программного обеспечения для закупочных процедур: доверенное ПО, стандартное российское ПО и иностранное ПО.
- Для статуса доверенного необходима совместимость как минимум с двумя операционными системами, отвечающими требованиям к доверенному ПО, за исключением случаев, предусмотренных правилами.

Вводится поэтапный переход к требованиям: для офисного ПО — с 01.09.2026, для других классов переходные сроки приходятся на 2027–2028 годы.

2. Реестр значимых разработчиков российского ПО

С 01.03.2026 вступил в силу приказ Минцифры России о создании реестра значимых разработчиков российского ПО²⁷.

Целью реестра является упорядочивание поддержки ключевых отечественных IT-компаний и регламентация создания значимых проектов по замещению иностранного софта с целью повышения технологического суверенитета.

Включение в реестр является важным условием участия в государственных закупках, получения господдержки и доступа к крупным проектам.

3. Продолжение грантового софинансирования проектов

В марте 2026 года Правительство РФ объявило о запуске нового отбора особо значимых проектов индустриальных центров компетенций, грантовое софинансирование для которых может достигать 50%.

При этом, согласно опросу, проведенному компанией Naumen в конце 2025 года среди бизнеса, более 70% российских компаний продолжали использовать зарубежное корпоративное ПО. Среди основных причин опрошенные выделяли отсутствие подходящей российской альтернативы (32% опрошенных) и высокую стоимость отечественных решений (16%). При этом ряд компаний рассчитывает на возвращение иностранных вендоров.

Ключевые выводы:

- Госполитика в рамках данного тренда направлена на формирование гарантированного спроса на отечественные IT-решения: приоритизация российского и евразийского ПО в госзакупках, продвижение отечественных пользовательских решений и др.
- Целью регуляторов является стимулирование создания решений, способных заменить зарубежные технологии не просто точечно, но на уровне ключевых технологических контуров. При этом значительная часть бизнеса продолжает использовать зарубежное ПО.

- Создание полного цикла производства и использования российского софта и электроники потребует не только регуляторных мер, но и создания собственной производственной базы, условия для развития которой на данный момент развиваются недостаточно быстрыми темпами.

Прогноз:

1. Усложнение доступа к мерам господдержки

Многоуровневая система допуска к преференциям в дальнейшем продолжит усложняться.

Наибольшее преимущество будут получать разработчики, проектирующие не точечные решения, а экосистемные проекты или способные вписываться в большинство разрабатываемых архитектур.

2. Запрос на формирование прозрачных критериев господдержки

С учетом того, что конкуренция между компаниями будет расти быстрее объемов господдержки, важным направлением для бизнеса должно стать обеспечение прозрачных и предсказуемых критериев ее предоставления.

7. Переход к более адресной модели государственной поддержки

Государственная поддержка IT-отрасли сохраняется, однако подход к ее предоставлению постепенно меняется. На фоне сокращения отдельных ранее действовавших налоговых преференций меры поддержки приобретают более адресный характер и в большей степени увязываются с выполнением дополнительных условий.

1. Корректировка налоговых льгот

В 2026 году для IT-компаний по-прежнему сохраняется ряд налоговых льгот, предусмотренных изменениями налогового законодательства прошлого года²⁸. Вместе с тем они с 01.01.2026 в значительной степени были скорректированы:

- Ставка налога на прибыль сохраняется на уровне 5% до 2030 года, но при соблюдении профильного условия о доле IT-доходов не менее 70%.
- Для IT-организаций с 2026 года действует повышенная ставка выплат по страховым взносам: 15% для выплат ниже предельной базы по страховым взносам (ранее 7,6%) и ставка 7,6% для выплат свыше базы (ранее — 0%).
- Скорректировано использование льготной ипотеки — теперь только в регионах (за исключением Москвы и Санкт-Петербурга) под 6% при выполнении условий (требования к зарплате, сохранение ставки при переходе в аккредитованную IT-компанию в срок 6 месяцев и др.).
- Запрещается одновременное применение льгот резидента «Сколково» и льгот для IT-компаний.

Также с 01.01.2026 появляется дополнительное условие для применения налогового коэффициента 2 для российского ПО: лицензионный или сублицензионный договор не должен предусматривать возможность передачи приобретенного права третьим лицам.

2. Инвестиционный налоговый вычет

Постановлением Правительства РФ²⁹ с 05.03.2026 корректируются параметры федерального инвестиционного налогового вычета, распространяемого в том числе на компании IT-сектора и телекоммуникаций. Среди изменений — передача права на вычет участникам группы компаний, а также уточнение условий и категорий налогоплательщиков.

Изменения распространяются на все правоотношения с 01.01.2026. Ключевое условие использования вычета остается прежним — средства от него должны направляться на развитие бизнеса.

3. Увеличение софинансирования особо значимых проектов (ОЗП)

В начале августа 2026 года премьер-министр М. Мишустин дал поручение пересмотреть механизм поддержки особо значимых проектов промышленных центров компетенций (ИЦК): грантовое софинансирование планируется увеличить с 50% до 80%.

При этом, по данным вице-преьера — руководителя Аппарата Правительства РФ Д. Григоренко на конец января 2026 года, в 2025 году

грантовую поддержку получили лишь 108 проектов малых предприятий в IT-сфере. В ходе «второй волны» выдачи грантов на реализацию особо значимых проектов ИЦК были отобраны 49 проектов, грантовую поддержку получили 17 из них.

Кроме того, согласно исследованию РУССОФТ, рост объема инвестиций в развитие российских софтверных компаний, составивший примерно 30–35% в 2024 году, в 2025 году сменился их сокращением на 37%.

Ключевые выводы:

- Господдержка IT-отрасли становится все более адресной, проектной и ориентированной на результат.
- При этом предоставление отрасли льгот напрямую увязывается с выполнением бизнесом взятых на себя обязательств, включая инвестиции, подготовку кадров и другие направления.

Прогноз:

1. Изменение приоритетов поддержки

Замедление роста отрасли создает основу для корректировки механизмов господдержки: от «стимулирования импортозамещения» к «стимулированию технологического развития и глобальной конкурентоспособности».

В результате критерии предоставления поддержки могут все больше учитывать не сам факт разработки российского ПО, а его технологическую значимость, потенциал коммерциализации и способность формировать долгосрочные конкурентные преимущества отрасли.

2. Концентрация господдержки и возможное снижение конкуренции

Дальнейшее повышение доли софинансирования ОЗП (с 50% до 80%) при сохранении узкого круга получателей повышает конкуренцию за попадание в этот контур и создает основания для периодического пересмотра критериев механизма в отдельных сферах.

Это может привести к формированию более узкого круга системно значимых получателей, тогда как для остальных компаний конкуренция за доступ к прямому бюджетному финансированию будет расти, а

сам доступ — все больше зависеть от соответствия государственным технологическим приоритетам.

¹ Критическая информационная инфраструктура (КИИ) — значимые информационные системы, сети, системы управления и базы данных, нарушение работы которых угрожает безопасности государства, экономике или гражданам. [↗](#)

² Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [↗](#)

³ Распоряжение Правительства РФ от 26.02.2026 № 360-р «Об утверждении перечня типовых отраслевых объектов критической информационной инфраструктуры Российской Федерации». [↗](#)

⁴ Постановление Правительства РФ от 13.04.2026 № 402 «Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере связи». [↗](#)

⁵ Постановление Правительства РФ от 16.01.2026 № 4 «Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры, функционирующих в области атомной энергии». [↗](#)

⁶ Постановление Правительства РФ от 06.02.2026 № 92 «Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры Российской Федерации в банковской сфере и иных сферах финансового рынка». [↗](#)

⁷ Постановление Правительства РФ от 07.03.2026 № 246 «Об утверждении отраслевых особенностей категорирования объектов критической информационной инфраструктуры Российской Федерации в сфере науки». [↗](#)

⁸ Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». [↗](#)

⁹ Федеральный закон от 09.04.2026 № 76-ФЗ «О внесении изменений в статью 274-1 Уголовного кодекса Российской Федерации». [↗](#)

¹⁰ Федеральный закон от 09.04.2026 № 77-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». [↗](#)

¹¹ Приказ ФСБ России от 25.12.2025 № 546 «Об утверждении Порядка обмена информацией о компьютерных атаках и компьютерных инцидентах между

субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты». [↗](#)

¹² Приказ ФСБ России от 26.12.2025 № 553 «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации». [↗](#)

¹³ Методический документ ФСТЭК России от 12.04.2026 «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах». [↗](#)

¹⁴ Приказ ФСТЭК России от 08.05.2026 № 137 «О внесении изменений в Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117». [↗](#)

¹⁵ Приказ ФСТЭК России от 27.02.2026 № 60 «О внесении изменений в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный приказом ФСТЭК России от 29 апреля 2021 г. № 77». [↗](#)

¹⁶ Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции». [↗](#)

¹⁷ Федеральный закон от 07.07.2025 № 214-ФЗ «О внесении изменений в часть четвертую Гражданского кодекса Российской Федерации». [↗](#)

¹⁸ Федеральный закон от 26.07.2026 № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации». [↗](#)

¹⁹ Указ Президента РФ от 26.02.2026 № 116 «О Комиссии при Президенте Российской Федерации по вопросам развития технологий искусственного интеллекта». [↗](#)

²⁰ Федеральный закон от 26.06.2026 № 211-ФЗ «О внесении изменений в Федеральный закон "Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации». [↗](#)

²¹ Федеральный закон от 31.07.2025 № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации». [↗](#)

²² Постановление Правительства РФ от 30.04.2026 № 504 «Об утверждении Правил формирования и ведения реестра посреднических цифровых платформ». [↗](#)

²³ Федеральный закон от 04.08.2026 № 295-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». [↗](#)

²⁴ Федеральный закон от 04.08.2026 № 279-ФЗ «О внесении изменений в Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». [↗](#)

²⁵ Приказ Минпросвещения России от 28.11.2024 № 838 «Об утверждении перечня средств обучения и воспитания, соответствующих современным условиям обучения...». [↗](#)

²⁶ Постановление Правительства РФ от 28.11.2025 № 1937 «О внесении изменений в некоторые акты Правительства Российской Федерации». [↗](#)

²⁷ Приказ Минцифры России от 25.12.2025 № 1246 «Об утверждении Порядка формирования и ведения перечня значимых разработчиков российского программного обеспечения». [↗](#)

²⁸ Федеральный закон от 28.11.2025 № 425-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации, отдельные законодательные акты Российской Федерации и признании утратившими силу законодательных актов (отдельных положений законодательных актов) Российской Федерации». [↗](#)

²⁹ Постановление Правительства РФ от 02.03.2026 № 210 «О внесении изменений в постановление Правительства Российской Федерации от 28 ноября 2024 г. № 1638». [↗](#)

Авторы



Александр Горохов
Аналитик, GR и оценка рисков
gorokhov@baikal-lobridge.ru



Валерий Афанасьев
Партнер, GR и оценка рисков
afanasyev@baikal-lobridge.ru



Все права защищены. Любое использование, распространение или цитирование материалов допускается только при наличии ссылки на источник.

Больше аналитических материалов вы найдете на сайте: baikal-lobridge.ru