

Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

- Как антимонопольные органы регулируют данные в конкуренции
- Как квантовые технологии становятся новой инфраструктурой
- Уровни доверия для облачных систем, на которых работают ИИ-системы госсектора

Мониторинг №6 (30) (Июнь 2026)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института Гайдара.

Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Солдаткина О.С., науч. сотр. Черновол К.А., науч. сотр. Голованова Д.А.

При частичном или полном использовании материалов ссылка на источник обязательна



Кто владеет данными, тот владеет рынком

В июне 2026 г. в США предложен к рассмотрению проект Закона об инновациях и выборе в интернете по регулированию конкуренции на цифровых рынках. Охватываются «системно значимые» платформы, годовой доход которых более **175** млрд долл., а аудитория – более **34%** населения США старше 12 лет, или **34%** домохозяйств (аналогично «гейткиперам» в ЕС).

Запреты введены при использовании данных:

- нельзя использовать непубличные данные продавцов для продвижения собственных товаров, например, выявлять наиболее успешные товары продавцов и выпускать собственные аналоги;
- нельзя ограничивать бизнес-пользователям доступ к их данным на платформы или мешать переносить и использовать их на других платформах.

Одним из способов превращения данных в источник монопольной власти являются слияния. В ЕС в июне 2026 г. обсуждался проект Руководства по слияниям, предлагающий учитывать не только возможности компаний удерживать цены, но и влияние слияний на доступ к данным, поскольку на цифровых рынках пользователи часто «платят» за бесплатные сервисы своими данными.

Объединенная после сделки компания может злоупотреблять своим положением: не предоставлять конкурентам доступ к критически важным данным, ухудшать условия доступа к данным. В итоге за счет получения монополии на данные по результатам сделки страдают компании, которые зависели от этих данных, и не могут получить к ним доступ из альтернативных источников.

В России примером такого поведения является кейс, когда в 2025 г. Wildberries закрыл от сторонних аналитических сервисов данные о товарах, ценах и рекламных ставках. Это не пример слияния, но он показывает, как контроль крупной платформы над данными может ограничивать конкуренцию и развитие компаний на смежных рынках: после того,

Как антимонопольные органы регулируют данные в конкуренции?

Автор: Мария Гирич

как Wildberries закрыл данные, начались сбои в аналитике.

При этом конкурентные преимущества от доступа к данным следует оценивать не только по их количеству, но и с учетом качественных характеристик – объема, разнообразия, скорости обновления, ценности и других параметров.

Чтобы снизить монополию крупных цифровых платформ на данные, регуляторы вводят требования по обеспечению их переносимости, заставляют делиться данными с конкурентами.

В июне 2026 г. Управление по конкуренции и рынкам Великобритании обязало Google разрешить пользователям передавать свои поисковые данные другим компаниям через специальный API.

А что дальше?

В России специальных правил оценки данных как фактора рыночной власти пока нет, однако ФАС в расследованиях уже учитывает данные как фактор конкурентного преимущества при оценке слияний и злоупотреблений доминирующим положением.

ВЧЕРА

2017–2025 гг.

Формирование специального регулирования цифровых рынков

Вводятся правила для доминирующих платформ: запрет продвигать собственные сервисы в ущерб конкурентам, дискриминировать контрагентов и препятствовать переходу пользователей на конкурирующие сервисы

СЕГОДНЯ

2026 г.

Признание данных источником рыночной власти

Страны начинают оценивать данные как фактор конкуренции

ЗАВТРА

Введение мер ограничения власти платформ над данными, включая доступ конкурентов к данным, интероперабельность и переносимость данных, контроль за объединением массивов данных при слияниях

Квантовый переход

Как квантовые технологии становятся новой инфраструктурой?

Автор: Диана Голованова

В июне 2026 г. в США принят [указ](#) о развитии квантовых инноваций. Планируется создание как минимум 1 квантового компьютера¹ для решения научных задач, которые невозможно выполнить на обычных компьютерах, а также развитие квантовых сенсоров и сетей.

1,9 млрд долл.

*составляет мировой рынок
квантовых технологий*

По данным ОЭСР, к концу 2025 г. квантовые технологии уже развивали 18 стран ОЭСР и ЕС, а с 2013 г. правительства разных стран выделили на их развитие около **55,7 млрд** долл.

Развитие квантовых технологий создает новые риски кибербезопасности. Станет возможным взлом криптографических алгоритмов и шифров, которыми защищаются переписка, платежи, данные. Эти риски мы рассматривали в [Мониторинге № 10 \(22\)](#).

Особый интерес представляют квантовые сенсоры, которые позволяют очень точно измерять параметры физического мира (например, время, давление) и поэтому используются там, где результат зависит от точности измерения, например, в добыче полезных ископаемых, навигации, космосе.

Однако при работе с такими сенсорами существует ряд рисков, связанных с доверием к данным: правильно ли работает сам сенсор, не были ли искажены его показания, безопасно ли произведено оборудование и нет ли уязвимостей в программах, на которых работает устройство.

Именно поэтому в июне 2026 г. в Австралии опубликовано [Руководство](#) для компаний по работе с квантовыми сенсорами. Выделены 4 риска:

Риск 1: на работу сенсора может влиять внешняя среда. Сенсоры очень чувствительны и могут считывать не только нужный сигнал, но и помехи, что снижает точность данных. Поэтому важно правильно выбрать место установки сенсора.

Риск 2: подмена данных. Злоумышленник может имитировать настоящий сигнал, добавить посторонний шум, чтобы сенсор передал неправильные данные. Поэтому необходимо проверять подлинность данных, например, через защищенную проверку сигналов² и систему выявления аномалий.

Риск 3: безопасность поставщиков и материалов. Для квантовых сенсоров нужны специальные материалы, детали, оборудование и прошивки (ПО). Поэтому на этапе производства или поставки есть риски, что в устройство попадут поддельные детали или вредоносные программы, которые в будущем повлияют на его работу. Компаниям рекомендуется проверять происхождение и подлинность оборудования и комплектующих.

Риск 4: безопасность программного обеспечения и прошивок. Уязвимости ПО могут нарушать работу сенсора и исказить передаваемые им данные. Поэтому необходимо регулярно проверять программы, через которые работает сенсор, своевременно их обновлять и устранять обнаруженные ошибки.

¹ Компьютер, который использует свойства малых частиц (т.е. то, как ведут себя атомы и другие маленькие частицы) для выполнения расчетов и может быстрее, чем обычный компьютер, решать сложные задачи.

² Например, с помощью электронной подписи, которая подтверждает, что сигнал отправил именно сенсор и данные не подменили.

А что дальше?

В России активно используются квантовые сенсоры, например, в геологоразведке компания [Геоскан](#) применяет квантовые магнитометры для поиска полезных ископаемых; в медицине компания [OLU](#) разрабатывает сенсоры для измерения слабых магнитных полей мозга; а в навигации компания [Сенсор Спин Технолоджис](#) разрабатывает квантовый гироскоп, который может определять, куда и с какой скоростью движется объект без спутников.

Регулирование квантовых технологий, включая квантовые сенсоры, в России пока разрабатывается. Однако в госпрограмме развития квантовых технологий [планируется](#) разработать 4 и внедрить 2 таких устройства к 2030 г. Подготавливаются также технические стандарты, ГОСТы для [квантовых коммуникаций](#) и [квантовых интернет вещей](#).

Поэтому важно развивать регулирование, особенно техническое, которое определяло бы, насколько точно должны работать квантовые сенсоры, как проверять их исправность, в каких условиях их можно использовать и как подтверждать корректность полученных от них данных.

ВЧЕРА

1980-е годы

Квантовые компьютеры начали развиваться как новый способ сложных расчетов

Квантовые компьютеры и системы развивались для решения задач, которые слишком сложны для обычных компьютеров (например, чтобы изучать строение молекул и химические реакции и создавать новые лекарства)

СЕГОДНЯ

2026 г.

Государства начинают создавать условия для применения квантовых технологий

Страны изучают риски, связанные с использованием квантовых сенсоров (вероятность сбора не тех данных в результате сверхчувствительности сенсоров к помехам; риск уязвимости, взлома, утечек данных из-за использования контрафактных компонентов, ПО)

ЗАВТРА

Введение общих правил безопасности квантовых технологий: переход на методы шифрования, устойчивые к квантовым компьютерам, установление требований к точности данных, к защите квантовых сенсоров

Облачно, возможен ИИ

ЕС готовит «уровни доверия» для облаков, на которых работают ИИ-системы госсектора

Автор:
Кирилл Черновол

В июне 2026 г. ЕС начал ужесточать требования к привлечению иностранных поставщиков облачных сервисов для работы государственных ИИ-систем.

Например, суд использует ИИ, созданный в ЕС, но работающий на облачной инфраструктуре иностранного провайдера. В результате судебные данные могут храниться за рубежом или быть доступны иностранному провайдеру, что создает риски утечек, потери доступа к сервису и пр.

В итоге ЕС представил проект Акта о развитии облаков и ИИ (CADA). Более **70%** облачного рынка ЕС контролируют всего **3** компании, и все они иностранные – Amazon, Microsoft, Alphabet. Государственная ИИ-инфраструктура становится зависима от иностранных облачных сервисов.

20%

*компаний разных стран
сталкивались с утечками данных
при использовании систем ИИ,
которые они не контролируют*

Чтобы оценивать, можно ли допускать иностранных провайдеров к закупкам, CADA вводит 4 «уровня доверия»: чем выше у провайдера уровень, тем более значимы для государства и общества функции, для которых он предоставляет облачные услуги:

- Уровень 1 - для некритичных функций (в ИИ не используются чувствительные данные, остановка сервиса не угрожает обществу). Пример: ИИ-системы для документооборота. Провайдер и облачная инфраструктура должны размещаться в ЕС;

- Уровень 2 - для функций с риском для публичного порядка (если есть чувствительные данные или сервис важен для работы госоргана). Пример: сервисы

управления медицинскими данными в государственных больницах. Персонал, здания, оборудование провайдера должны быть в ЕС. Иностранная материнская компания не должна иметь возможности приказать «дочке» из ЕС отключить сервис;

- Уровень 3 - для более значимых функций (правоохранительная, судебная деятельность, где данные составляют гостайну). Персонал должен иметь гражданство ЕС. Компании, подконтрольные иностранным лицам, не могут иметь уровень 3 или выше;

- Уровень 4 - для самых критичных функций (оборона, национальная безопасность и пр.). Поставщик не должен контролироваться иностранными лицами, вся поддержка сервиса и доступы к данным должны предоставляться только на территории ЕС.

Несмотря на ужесточение требований, Amazon, Microsoft, Alphabet и прочие иностранные облака могут участвовать в закупках уровней 1–2 через европейские «дочки» - у Amazon Web Services и Google Cloud они есть.

В России в июне 2026 г. в Госдуму РФ был внесен (принят в июле) проект ФЗ о поддержке развития ИИ, в котором подход отличается от ЕС: хранение данных государственных ИИ-систем должно обеспечиваться в центрах анализа данных, принадлежащих российским юрлицам. При этом в российском законопроекте нет деления по критичности госсистем, для которых потребовались бы разные «уровни доверия», как в ЕС.

Различаются и определения контроля. В России нельзя, чтобы более 50% компании принадлежало иностранцам. В ЕС контроль – это возможность оказывать «решающее влияние» на работу компании, в том числе через ключевые для нее контракты или иностранных топ-менеджеров. Подход более широкий, чем в России.

А что дальше?

В ЕС функционируют около **59** облачных кластеров дата-центров³, при этом **83%** из них принадлежат поставщикам не из стран ЕС.

К 2030 г. ЕС планирует утроить собственные мощности дата-центров и полностью покрыть потребности в облачных вычислениях для ИИ к 2035 г.

В России планы по развитию дата-центров пока не приняты, но планируется не допускать компании с иностранным участием до обслуживания инфраструктуры для государственного ИИ.

ВЧЕРА

2020–2025 гг.

Китай: планы по созданию национальной системы больших ЦОД
США: «миссия Genesis»
ЕС: Регламент о создании национальных «гигафабрик ИИ»

Страны разрабатывают нормы и планы по самообеспечению вычислительными мощностями для ИИ

СЕГОДНЯ

июнь 2026 г.

ЕС: регламент CADA
Россия: проект ФЗ об ИИ

Страны ограничивают доступ иностранных поставщиков облачных вычислений для ИИ-систем в госсекторе и для критической инфраструктуры

ЗАВТРА

Защита цифрового суверенитета через ограничение иностранных облаков для государственных ИИ-систем: требования локализации и размещения оборудования на территории страны и др.

³ [AWS – 6, Microsoft Azure – 12, Google Cloud – 11, Oracle – 9, Exoscale – 6, IBM Cloud – 2, Alibaba Cloud – 2, Tencent Cloud – 1, OVHcloud – 7, Hetzner – 3.](#)

DIGEST

DIGEST

Новости **в июне 2026 г.**, которые нам показались интересными¹.

- В Великобритании Орган по конкуренции и рынкам заставляет Apple делиться технологией NFC¹ в iPhone. Ранее Apple давала доступ к NFC исключительно для собственных сервисов. Потребители были вынуждены пользоваться на iPhone только Apple Pay и Apple Wallet для бесконтактной оплаты. Ожидается, что после предоставления доступа NFC появятся сервисы с оплатой цифровыми валютами и стейблкоинами.
- В России владельцев сайтов будут наказывать на 500–700 тыс. руб., если те дают пользователям регистрироваться или заходить на сайт любым способом, кроме как разрешено в законе – штраф будет, например, за регистрацию через Gmail.
- Антимонопольный орган Кореи опубликовал доклад о влиянии алгоритмического самопредпочтения платформ на выбор потребителей. Выявлено, что, если платформа искусственно поднимает собственный товар в поисковой выдаче, вероятность его покупки увеличивается на **34%**, а вероятность покупки товара конкурента снижается на **32%**.



¹ С 2025 г. Институт Гайдара разрабатывает цифровую платформу анализа новостей в России и в мире по тематике регулирования цифровой экономики – DigiReg. Представленные новости отобраны экспертами в том числе на основе анализа данных платформы.

¹ Near Field Communication (NFC) – совокупность протоколов беспроводной связи малого радиуса действия, широко используемых в мобильных устройствах, например, при оплате телефоном через платежный терминал.