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

- **Конкуренция при трансфере технологий**
- **Налоговое выравнивание цифровой торговли**
- **Токенизация финансового рынка**
- **Риски квантовых компьютеров**
- **Трансграничная передача данных**
- **Защита пользователей «интернета вещей»**
- **Персональные данные для ИИ**

Мониторинг №10 (22) (Октябрь 2025)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института экономической политики имени Е. Т. Гайдара (Института Гайдара).

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

«Кто дожил до Октября,
Поработал он не зря,
В Октябре, как в Марте, в нас
Живо сердце, ум погас.»
К. Бальмонт

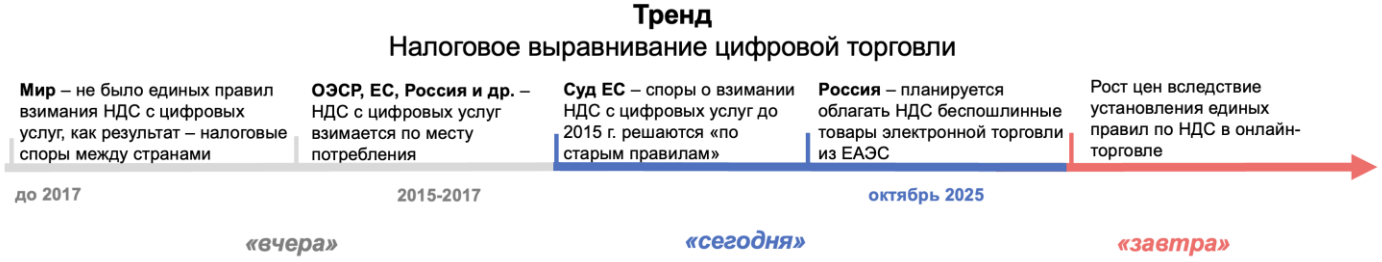
В октябре 2025 г. можно выделить 7 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Конкуренция при трансфере технологий

В октябре 2025 г. в ЕС представлен проект регламента, определяющий условия, при которых соглашение о трансфере технологий между компаниями не будет признаваться антиконкурентным. Россия предложила ограничить антимонопольный иммунитет для правообладателей интеллектуальной собственности.

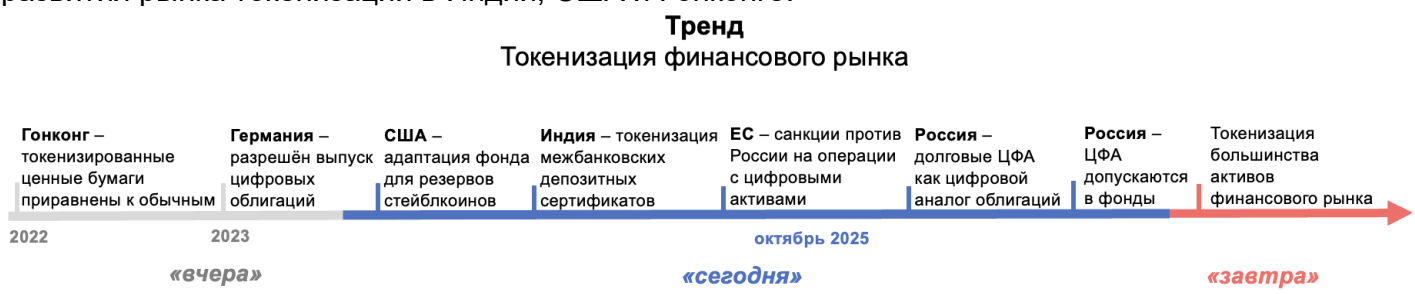
Тренд № 2. Налоговое выравнивание цифровой торговли

В октябре 2025 г. Суд ЕС признал, что НДС с онлайн-услуг, оказанных до 2015 г., взимается по месту нахождения поставщика, а после 2015 г. – пользователя. Это тренд, связанный с переходом стран к единым правилам обложения НДС онлайн-услуг, разработанным ОЭСР. В России Минфин планирует облагать НДС купленные онлайн товары из стран ЕАЭС.



Тренд № 3. Токенизация финансового рынка

В октябре 2025 г. в Государственную Думу России внесены законопроекты, направленные на развитие рынка цифровых финансовых активов (ЦФА): фондам разрешат приобретать такие активы, в законодательстве появится новый актив ЦФА - облигация. Изменения проходят на фоне развития рынка токенизации в Индии, США и Гонконге.



Тренд № 4. Риски квантовых компьютеров

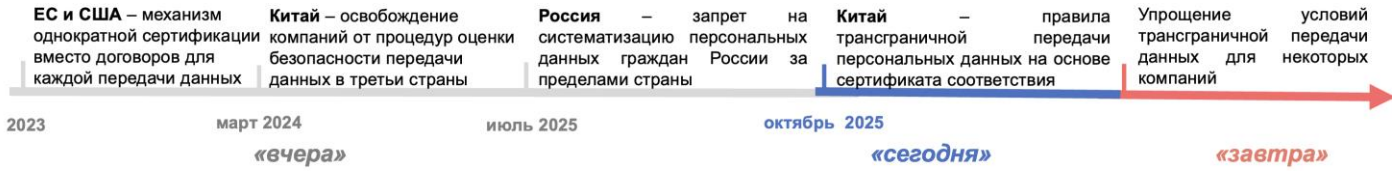
В октябре 2025 г. Сингапур выпустил проект руководства по внедрению «квантово-устойчивых решений» против утечек чувствительных данных, сбоев критической инфраструктуры при распространении квантовых компьютеров. Разработан Индекс готовности к квантовым вычислениям.

Тренд
Риски квантовых компьютеров

Тренд №5. Трансграничная передача данных

В октябре 2025 г. Китай утвердил правила упрощенной трансграничной передачи персональных данных: вместо прохождения регулярной оценки безопасности экспорта данных можно однократно пройти сертификацию безопасности для передачи данных в течение 3 лет.

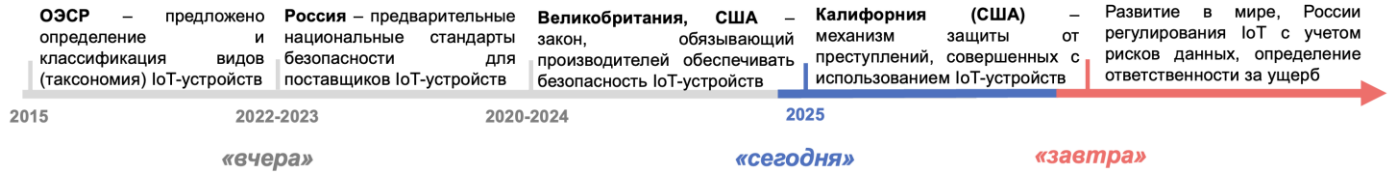
Тренд
Трансграничная передача данных



Тренд 6. Защита пользователей «Интернета вещей»

В октябре 2025 г. в США принят закон о защите пострадавших, которым злоумышленники наносят вред через устройства «интернета вещей».

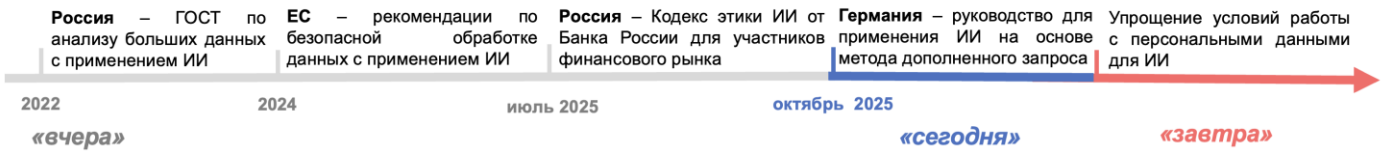
Тренд
Защита пользователей «интернета вещей»



Тренд 7. Персональные данные для ИИ

В Германии разработано Руководство для организаций, применяющих технологии ИИ с методом контекстуального уточнения пользовательских запросов.

Тренд
Персональные данные для ИИ



Также в России в октябре 2025 г. были **урегулированы платные подписки на цифровые сервисы.** Теперь у потребителя появилось право[1] отказаться от платных подписок, удалить сведения о банковской карте. А приложения и сайты не вправе без разрешения потребителя списывать деньги, если потребитель отказался от подписки. По исследованиям, 50% пользователей подписаны в России на услуги, не соответствующие заявленному предложению

[1] Федеральный закон от 15.10.2025 № 376-ФЗ "О внесении изменения в статью 16-1 Закона Российской Федерации "О защите прав потребителей"

по подписке[2]. Из них половина пользователей обращалась с просьбой отменить подписку, но большинству не удалось вернуть средства. В ЕС до 10% потребителей сталкивались с такими списаниями[3].

Таким образом, законопроект минимизирует риски незаконных списаний, однако нормы можно было бы дополнить предупреждением, что после «бесплатной пробной» версии подписка становится платной, и установления понятного для потребителя механизма отписки и пр. Также интересен опыт ЕС, где в течение 2-х недель с момента покупки потребитель может оформить «возврат» подписки, вернув деньги за неиспользованный период подписки.

[2] https://nemkin.ai/tpost/785uhpmso1-podpiski-kotorie-nam-navyazali-millioni
[3] https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en

Ключевые аспекты

1. Конкуренция при трансфере технологий

Опыт ЕС

В октябре 2025 г. ЕС представил проект правил, автоматически освобождающих отдельные соглашения о передаче технологий[4] от признания антиконкурентными[5] - пока не закончился срок действия прав интеллектуальной собственности или ноу-хау не стало общеизвестным. Освобождение действует, если соглашение заключают конкурирующие предприятия с совокупной долей рынка не более 20%, а если предприятия не конкурируют – то до 30%. Освобождение не применяется, если содержит обязанность лицензиата покупать определённые товары или компоненты у правообладателя.

Если предприятия конкурируют, то соглашение не должно:

– ограничивать право сторон самостоятельно определять цены при продаже продукции;

– ограничивать объемы производства;

– быть направлено на раздел рынков или клиентов (кроме случаев, когда, например, лицензиат производит товары только для себя или для одного клиента);

– ограничивать право лицензиата использовать собственные права на технологию, осуществлять НИОКР (если только ограничение реально необходимо, чтобы не утекло ноу-хау третьим лицам).

Если стороны соглашения не конкурирующие, то соглашение не должно:

– ограничивать сторону в определении цены;

– ограничивать территорию или клиентов, где лицензиат может осуществлять «пассивные»[6] продажи клиентам.

В соглашениях запрещено требовать от лицензиата предоставлять лицензиару или третьему лицу исключительную лицензию или передавать усовершенствования технологии или разработки лицензиата.

Представленные меры позволяют компаниям свободнее заключать соглашения о передаче технологий, стимулируя распространение инноваций, с попыткой не допустить, чтобы технологиями прикрывали антиконкурентные соглашения и скрытые картели, а патенты и ноу-хау не превращались в инструмент раздела рынков, фиксации цен, исключения конкурентов, блокирования третьих лиц.

Опыт России

В России запрет на антиконкурентные соглашения, а также нормы о злоупотреблении доминированием не применяется по общему правилу к соглашениям о предоставлении, отчуждении прав интеллектуальной собственности, что потенциально затрагивает и трансфер технологий. Однако в октябре ФАС опубликовало законопроект, который может снять такой иммунитет[7]. Предлагается ограничить случаи действия иммунитета, которые будут установлены правительством. Таким образом, подход ЕС в смягчении действующих строгих норм, в России, наоборот, снижение существующих привилегий.

Количество соглашений о трансфере технологий будет увеличиваться: ежегодный рост рынка на 11,7% до 2035 г.[8] Можно ожидать тренд на развитие гибридного регулирования: стимулирования свободы соглашений трансфера технологий, но с усиленным мониторингом соглашений с высоким риском ограничения конкуренции, особенно за крупными компаниями.

2. Налоговое выравнивание цифровой торговли

Опыт ЕС

В октябре 2025 г. Суд ЕС вынес решение по спору о взимании НДС при покупках «внутри приложения»,

[4] Соглашение о передаче технологий – это лицензионное соглашение о правах на технологии, либо уступка прав на технологии, заключенные между предприятиями для производства продукции лицензиатом или его субподрядчиками. Передаются права на ноу-хау (секрет производства), а также патенты, полезные модели или дизайн, топографии полупроводниковых изделий, патенты на лекарства, авторские права на ПО и др.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505024

[6] «Активные продажи» - активное привлечение клиентов посредством посещений, писем, электронных писем, звонков или других средств прямой коммуникации или посредством целевой рекламы и продвижения, офлайн или онлайн,
«Пассивные продажи» - продажи, осуществляемые в ответ на запросы отдельных клиентов, при этом продажа не была инициирована путем активного нацеливания на конкретного клиента или территорию, а также продажи, осуществляемые в результате участия в государственных закупках или ответа на частные приглашения к участию в торгах.

[7] https://regulation.gov.ru/projects/159126/

[8] https://www.researchnester.com/reports/technology-licensing-market/8210

совершённых до 2015 г. через магазин приложений, управляемый компанией в Ирландии. Немецкая налоговая служба после 2015 г. проверяла немецкого разработчика мобильных игр XYRALITY, продававшего контент внутри своих приложений через AppStore, владелец которого зарегистрирован в Ирландии. Немецкие налоговики решили, что хотя платежи шли через Ирландию, фактические покупатели находились в Германии, поэтому компания должна была уплатить немецкий НДС.

Налоговое ведомство Германии приняло позицию, что магазин приложений AppStore был лишь посредником по проведению платежей, а поставщиком для пользователей был немецкий разработчик – значит, НДС должен начисляться в Германии. Дополнительно ведомство приводило довод, что XYRALITY указывалась в подтверждениях покупок как поставщик услуг, что якобы подтверждало обязанность компании платить НДС. XYRALITY, напротив, утверждала, что AppStore действовал «от своего имени, но по поручению» компании, и потому именно AppStore считается поставщиком для конечных пользователей, а разработчик только оказывает услугу площадке. Следовательно, НДС должен платиться в Ирландии, а не в Германии.

Суд ЕС сослался на ст. 28 Директивы ЕС об НДС:[9] если лицо участвует в оказании услуги «от своего имени, но по поручению» другого, то для целей НДС оно считается получившим и затем оказавшим ту же услугу – признаётся поставщиком перед конечным покупателем. Суд выделил в деле 2 факта поставки услуг (контента): от разработчика в AppStore – это сделка B2B, и местом её совершения будет Ирландия, потому что там находится платформа, и из AppStore пользователю – это B2C-продажа, и она определяется по месту нахождения поставщика, то есть также в Ирландии. Значит, НДС подлежит уплате в Ирландии, а не в Германии.

Следует отметить, что ОЭСР с 2017 г. закрепляет принцип налогообложения по месту потребления: НДС на международные услуги должен поступать туда, где происходит конечное потребление. Для цифровых услуг, приобретаемых физическими лицами (B2C), это страна проживания покупателя, а для B2B-поставок – страна нахождения покупателя. При определении сторон сделки ОЭСР предлагает исходить из того, кто указан как покупатель и продавец в договоре или счете. При этом прямое предоставление услуги третьему лицу или оплата третьим лицом не меняют ни того, кто считается поставщиком, ни место налогообложения. То есть Суд ЕС применил действовавшую в спорный период (2012-2014 г.) в ЕС модель «по месту поставщика» (Ирландия как юрисдикция AppStore), а ОЭСР описывает модель «по месту потребителя».

Сейчас сформулированный ОЭСР подход является общепринятым в мире, до этого страны собирали НДС с цифровых услуг по-разному. Поэтому возникали налоговые споры между бизнесом и властью, а также между странами. Рассмотренное дело показывает, что эта проблема актуальна до сих пор, хотя единый подход ОЭСР разработан еще 8 лет назад. Цифровым компаниям важно помнить: претензии по НДС по цифровым услугам в России до 2017 г. (в ЕС – до 2015 г.) должны рассматриваться с учетом действовавших тогда правил определения юрисдикции. Где-то НДС подлежал уплате по месту нахождения получателя услуги (пользователя), где-то – поставщика (разработчика или владельца платформы).

Опыт России

В России до 2017 г. онлайн-услуги иностранных компаний российским физическим лицам в большинстве случаев не облагались российским НДС: для них не срабатывало общее правило «по месту покупателя» (ст.148), и местом реализации считалось место деятельности иностранного исполнителя — за пределами РФ (ст. 161 НК РФ). Этот пробел закрыли с 2017 г., когда начала действовать статья 174.2 НК РФ, по которой теперь применяется описанный выше подход ОЭСР.

Минфин России в октябре 2025 г. разработал законопроект по НДС на товары электронной торговли (с маркетплейсов) из стран ЕАЭС. Ставки будут расти постепенно: в 2027 г. – 5%, в 2028 г. -– 10%, в 2029 г. -–

[9] Директива от 28 ноября 2006 г. № 2006/112/ЕС

15%, а с 2030 г. –- 20%. Сейчас, если товар ввозится в Россию почтой или курьером для личного пользования, и его стоимость не превышает беспошлинный порог ЕАЭС, НДС не платится[10]. Поэтому товары на маркетплейсах бывает покупать выгоднее, чем офлайн. Введение НДС может привести к росту цен на товары на интернет-площадках, плательщики НДС (платформы или продавцы) будут включать сумму НДС в цену.

Взимание НДС на товары в электронной торговле – глобальная практика (уже внедрили более 40 стран[11]). Товары дорожают на величину стандартной ставки налога – около 19,3% по странам ОЭСР,[12] а спрос на покупки снижается на 50%[13].

Глобально система международного налогообложения в цифровой торговле в мире будет приводиться к единому своду правил. На сегодняшний день более 100 стран уже провели реформы по НДС для трансграничной электронной торговли на базе стандартов ОЭСР, ещё свыше 30 готовятся внедрять[14]. Проблема международного налогообложения товаров и услуг, продаваемых онлайн, не решена до конца – например, остаются вопросы, как странам распределять прибыль «цифровых гигантов» и по каким правилам собирать отчетность для НДС с компаний[15].

3. Токенизация финансового рынка

Опыт России

В октябре 2025 г. в Госдуму внесен законопроект[16] о новом виде цифровых активов – долговых ЦФА. Это цифровой аналог облигаций: инвестор предоставляет эмитенту деньги и получает право на их возврат с процентами. Сейчас выпуск облигаций с использованием инструмента ЦФА невозможен: можно выпустить ЦФА на денежное требование или же ЦФА на уже выпущенные традиционные облигации. Законодатель же предлагает допустить возможность выпуска финансового инструмента – облигации сразу в токенизированном виде *(native tokens)*. Такой подход закрепляет использование ЦФА как инструмента долгового финансирования: фиксированные условия и график выплат позволяют регулировать их по принципам, применяемым к традиционным долговым инструментам.

Предложение повлияет и на оценку рисков банков при формировании резервов: Базельский комитет считает, что ЦФА, выпущенный на облигацию, имеет больший риск для банка, чем ЦФА – облигация. На долговые ЦФА сегодня приходится 88% российского рынка цифровых финансовых активов. Стоит ожидать, что после принятия поправок, новый актив станет доминирующим на рынке ЦФА[17].

Также в октябре 2025 г. в Госдуму был внесен законопроект[18], который позволяет инвестиционным фондам приобретать ЦФА на тех же условиях, что и акции или облигации. Ранее фонды фактически не могли включать ЦФА в состав своих активов, поскольку не было закреплённого механизма депозитарного учёта. Поправки вводят такой механизм (включая режим номинального держателя), что открывает ЦФА доступ к институциональным инвесторам и делает операции с ними сопоставимыми с обращением классических ценных бумаг. Для брокеров и управляющих компаний закрепляются те же требования по защите интересов клиентов, что и на рынке ценных бумаг. Это делает покупку ЦФА для частных инвесторов прозрачной и контролируемой, как и приобретение традиционных финансовых инструментов. Однако регулятор сохраняет ограничения и инвесторские тесты, чтобы розничные инвесторы могли приобретать ЦФА с учётом своего опыта и допустимого уровня риска.

Отметим, что развитие российского законодательства происходит на фоне новых санкций со стороны ЕС, которые коснулись и рынка криптоактивов. Новый пакет санкций[19] запретил европейским и зарубежным криптоплатформам обслуживать российских пользователей и компании. Ограничения также распространяются на операции с

[10] На сегодня пошлины и НДС не взимаются с товаров стоимостью до 200 евро и весом до 31 кг, но с 2026 г. планируется снижение этого порога до 100 евро, с 2027 г. - до 50 евро, а в 2030 г. беспошлинный порог будет отменен.
[11] https://www.oecd.org/en/publications/tax-policy-reforms-2025_de648d27-en/full-report/tax-policy-reforms_c57e058c.html
[12] https://www.oecd.org/en/publications/2024/11/consumption-tax-trends-2024_57c7322a.html
[13] https://ideas.repec.org/a/eee/pubeco/v239y2024ics0047272724001804.html
[14] https://www.oecd.org/en/topics/sub-issues/vat-policy-and-administration.html
[15] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/11/consumption-tax-trends-2024_57c7322a/dcd4dd36-en.pdf
[16] https://storage.consultant.ru/site20/202510/24/pr_241025_142.pdf
[17] https://cbr.ru/Collection/Collection/File/55196/review_2024.pdf
[18] https://storage.consultant.ru/site20/202510/09/pr_091025_411.pdf
[19] https://eur-lex.europa.eu/eli/reg/2025/2033/oj

рядом цифровых активов, включая рублёвый стейблкоин A7A5[20].

Опыт Гонконга, Германии, Индии, США

Необходимо отметить, что меры, реализуемые в России в октябре, не являются уникальными – аналогичный подход уже применяется в ряде стран. Так, в Гонконге Комиссия по ценным бумагам и фьючерсам приравняла токенизированные ценные бумаги к обычным и установила для них те же требования по защите инвесторов, раскрытию информации и безопасному хранению. Аналогичный подход реализован и в Германии, где закон об электронных ценных бумагах разрешил выпуск долговых инструментов в цифровой форме и приравнял их к традиционным облигациям при сохранении требований к защите инвесторов и раскрытию информации.

В Индии в октябре 2025 г. Резервный банк запустил пилотный проект[21] по токенизации депозитных сертификатов[22] – краткосрочных долговых инструментов межбанковского рынка. Это ускоряет расчёты и снижает операционные риски, что перекликается с российским акцентом на цифровых облигациях и создании инфраструктуры их обращения.

В развитии рынка токенизации начинают принимать участие крупные инвестиционные фонды мира. В октябре 2025 г. компания BlackRock[23] адаптировала один из своих фондов[24] под требования GENIUS Act[25], дав возможность эмитентам стейблкоинов приобретать паи этого фонда для запуска проекта.

Таким образом, в мире формируется тренд на токенизацию традиционных финансовых активов. Ожидается, что этот тренд будет усиливаться по мере развития инфраструктуры и расширения практики использования таких инструментов. По оценкам, к 2030 году объём таких активов может достигнуть от 4–5 до 16 трлн долл.[26][27], и наибольший рост ожидается в сегменте инструментов для привлечения и размещения денежных средств, включая цифровые аналоги облигаций.

4. Риски квантовых компьютеров

Опыт Сингапура

В октябре 2025 г. Сингапур выпустил проект Руководства по внедрению в организациях «квантово-устойчивых решений» для преодоления рисков появления квантовых компьютеров (например, рисков потери данных, кражи криптовалют и др.). Так, день «Q» - начало отсчета, когда распространятся квантовые компьютеры (ближайшие 5–10 лет), способные взламывать криптографические методы шифрования данных сети[28] (до 100 млн раз быстрее классических компьютеров[29]), менее уязвимое шифрование (как блокчейн-сети), критическую инфраструктуру (банки, государственные системы).

Квантовые угрозы создают риски утечек как персональных данных, так и коммерческой, государственной тайны, в том числе риск угрозы «собери сейчас, расшифруй потом»[30], а также к сбоям в работе систем (если перехвачен доступ к системам диспетчерского управления за промышленными и инженерными объектами, ЖКХ). В итоге скомпрометированные элементы доступа (как цифровые подписи) приводят к риску финансовых манипуляций (например, кража денег, криптовалют в транзакциях) или изменению данных. Для предотвращения угроз организации могут внедрять «квантово-устойчивые решения». Нужно:

1. Оценить риски квантовых угроз с учетом приоритетов ведения бизнеса[31] и

[20] Рублевый стейблкоин, выпускаемый российской компанией A7 в Кыргызстане
[21] https://www.business-standard.com/economy/news/rbi-deposit-tokenisation-pilot-cbdc-wholesale-digital-tokens-oct8-125100700532_1.html
[22] Краткосрочные ценные бумаги, с помощью которых банки занимают деньги друг у друга под фиксированную ставку.
[23] Инвестиционная компания, управляющая разными типами фондов и активов для частных и институциональных инвесторов.
[24] https://www.businesswire.com/news/home/20251016818364/en/BlackRock-Introduces-40-Act-2a7-Money-Market-Fund-in-GENIUS-aligned-Form
[25] Закон в США, который регулирует выпуск стейблкоинов и определяет в каких активах должны храниться их резервы. Мы подробно рассказывали о нем в Мониторинге № 5 (17).
[26] https://www.citigroup.com/global/insights/money-tokens-and-games
[27] https://web-assets.bcg.com/1e/a2/5b5f2b7e42dfad2cb3113a291222/on-chain-asset-tokenization.pdf
[28] Технические методы сети, которые используются, чтобы сделать данные недоступными для сторонних пользователей (например, онлайн-транзакций, сообщений).
[29] https://www.proskauer.com/blog/blockchain-and-quantum-computing
[30] «Собери сейчас, расшифруй позже» — это метод, при котором злоумышленники получают данные в зашифрованном виде уже сейчас с намерением расшифровать их в будущем, когда появится квантовый компьютер. Наиболее уязвимыми будут ценные данные с длительным сроком хранения, поскольку их расшифровка в будущем может дать существенные преимущества, например, личные финансовые данные и медицинские записи.
[31] Организации могут использовать установленные стандарты для анализа влияния на бизнес, планирования непрерывности бизнеса и количественной оценки рисков (например, ISO/TS 22317 (анализ влияния рисков на бизнес), ISO 22301 (системы управления непрерывностью бизнеса), NIST SP 800-34 (планирование действий в чрезвычайных ситуациях).

затронутых данных (какие данные наиболее уязвимы к угрозам, классифицировать их)[32];

2. Организовать корпоративную систему управления, разработать план внедрения новых стандартов шифрования;

3. Менять алгоритмы шифрования данных на устойчивые к атакам квантовых компьютеров (например, по стандартам - FIPS 203, 204, 205[33]), проводить регулярное тестирование;

4. Проводить обучение сотрудников;

5. Оценивать риски квантовой безопасности при взаимодействии с поставщиками (третьими лицами).

Для оценки развертывания организациями таких систем Сингапур разработал чек-лист для самостоятельной проверки – Индекс готовности к квантовым вычислениям (QRI). Например, какой объем обрабатываемых ценных данных может быть затронут? Проводится ли инвентаризация всех криптографических активов для шифрования информации в системе? Всего 4 уровня оценки QRI: где 0 – процесс не запущен, организация не начала квантово-безопасную миграцию[34,35], а 3 – организация внедряет квантово-устойчивые решения, запущен процесс постоянного мониторинга.

Опыт России

Работа по разработке стандартов постквантовой криптографии осуществляется Техническим комитетом по стандартизации (ТК26). Последний стандарт опубликован 17.09.2025 г. и определяет систему понятий в области криптографической защиты информации[36].

Стоит ожидать, что далее в мире (и России) регуляторы будут активнее вводить требования для своих организаций по переходу на постквантовую криптографию (например, сроки, когда национальные организации должны полностью внедрить квантово-устойчивые стандарты шифрования). США и Великобритания нормативно определили срок в 2035 г. в части завершения поэтапного перехода организаций, а Австралия – 2030 г.[37] Стоит также ожидать в России принятие полноценного стандарта постквантовой криптографии.

5. Защита пользователей «интернета вещей»

Опыт Калифорнии (США)

В октябре 2025 г. в США подписан закон о защите пострадавших от устройств «интернета вещей». К таким устройствам относятся, например, технологии «умного дома» (датчики автоматического включения света, управление температурой, камеры видеонаблюдения и т. д.). 97% программ по борьбе с домашним насилием в США сообщают, что устройствами IoT можно злоупотреблять как инструментом эмоционального или физического насилия, угроз. Злоумышленники, например, взламывают мобильные приложения, чтобы дистанционно управлять предметами быта (например, периодически включают или выключают свет, меняют коды от цифрового замка в двери каждый день), следят за своими жертвами[38].

Закон Калифорнии обязывает компании – «менеджеров» учетных записей устройств IoT[39] создавать механизм, позволяющий в течение 2 дней блокировать доступ злоумышленника к учетной записи (или сбросить до заводских настройки доступа) в случае подачи пострадавшим «запроса на защиту устройства». Причем компании запрещено требовать от пострадавшего каких-либо дополнительных условий (в том числе. оплаты/штрафов). В рамках запроса пострадавшему необходимо подтвердить владение устройством, факт совершения через устройство незаконных деяний.

Опыт России

В России принят ряд предварительных национальных стандартов безопасности для IoT, например, ПНСТ № 642–2022 (общие положения в сфере промышленного «интернета вещей»), ПНСТ № 818–2023 (перечень основных базовых компонентов

[32] Например, такие данные: общедоступные публичные или конфиденциальные секретные данные.
[33] Три международных базовых постквантовых криптографических стандарта от Национального института стандартов и технологий США, которые предлагают алгоритмы шифрования, устойчивые к взлому квантовых компьютеров.
[34] 1 уровень - Организация приступила к изучению квантовой угрозы и начала работу по внедрению.
[35] 2 уровень - Организация применяет общеорганизационный подход для внедрения квантово-устойчивых решений.
[36] ГОСТ р 34.14-2025. Информационная технология. Криптографическая защита информации. Термины и определения.
[37] https://blog.cloudflare.com/pq-2025/
[38] В 2018 г. New York Times публиковал интервью с 30 жертвами с жертвами насилия, пострадавших от IoT https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
[39] Программы, которые управляют доступом пользователей к устройствам, через которые пользователь проходит идентификацию и получает учетную запись, например программа «менеджер умного дома».

систем IoT) и другие. В части вреда, причиненного IoT-устройством, распространяется общее регулирование Закона «О защите прав потребителей» – ответственность на изготовителе устройства, если изготовитель не докажет, что устройство использовалось не по инструкции, и нарушение со стороны покупателя.

Количество устройств IoT в мире может вырасти на 69% к 2034 г. с 2025 г. (+20 млрд новых устройств)[40]. Текущее регулирование в России не учитывает отдельные риски безопасности (минимизация собираемых данных; ответственность за ущерб IoT устройства). Можно прогнозировать, что в перспективе как в мире, так и в России будет расширяться регулирование IoT-устройств с учетом различных типов оборудования и устраняющее риски, а также законодательное расширение мер защиты пользователей.

6. Трансграничная передача данных

Опыт Китая

В октябре 2025 г. Китай утвердил правила, упрощающие трансграничную передачу данных через сертификацию. По общему правилу передача данных в третьи страны возможна при получении разрешения на такую передачу. Для этого проводится оценка безопасности экспортной операции Государственным управлением по кибербезопасности. Новая процедура сертификации позволяет компаниям передавать данные за рубеж на основании сертификата, подтверждающего, что компания принимает со своей стороны все меры, чтобы данные и при передаче, и при обработке в третьей стране были в безопасности. Процедура освобождает китайские компании от необходимости получения разрешения на каждую отдельную операцию с данными. Однако процедура доступна компании, которая должна:

– не быть оператором критической информационной инфраструктуры;

– передавать от 100 тыс. до 1 млн записей персональных данных или 10 тыс. записей чувствительных данных в год;

– не передавать данные, классифицируемые как «важная информация», нарушение безопасности создает риски для национальной безопасности и экономики.

Сертификация действует 3 года и ориентирована на малый бизнес с ограниченными объемами передач. Тем не менее даже компании с сертификатом подлежат государственному надзору, например, внеплановым проверкам.

Опыт России

В России установленный порядок трансграничной передачи данных не предусматривает упрощений для отдельных категорий операторов данных. Сложность прохождения уведомительной процедуры де-факто дифференцируется в зависимости от страны назначения экспорта персональных данных: для стран, не входящих в список Роскомнадзора о признании правового режима защиты данных адекватным российскому, оператору данных необходимо готовить дополнительные документы о наличии правовых гарантий защиты данных после их передачи в третью страну. Поэтому сегодня российские компании не получают регуляторной поддержки для развития бизнеса, предполагающего трансграничный оборот данных. Оборот данных является ключевым условием ведения бизнеса в цифровой экономике. В 2025 г. на цифровую экономику приходится уже 24% мирового ВВП. Причем к 2026 г. ежемесячный поток данных достигает 690 гигабайт в месяц, что в 3 раза превосходит показатель 2020 г.[41] Таким образом, сохранение текущего регуляторного режима создает риски потери конкурентоспособности цифровых российских компаний.

7. Персональные данные для ИИ

Опыт Германии

В октябре 2025 г. принято Руководство по защите данных для компаний, использующих технологии генеративного ИИ на основе метода поиска и дополненной генерации[42] «RAG» – когда запрос

[40] https://www.statista.com/topics/2637/internet-of-things/?srsltid=AfmBOooIhcQhRchscIMF9cdcgqkPfvr0NJrUZQ9ebDXIlHZYn4AfncIS#topicOverview

[41] https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2025/navigating-cross-border-data-flows.pdf

[42] Retrieval Augmented Generation

пользователя дополняется контекстом, уточняется, прежде чем запрос поступает в ИИ для генерации ответа. Руководство предназначено для организаций, обрабатывающих персональные данные через системы RAG, включая использование встроенных моделей ИИ и векторные базы[43] данных. Выделяется 7 принципов работы:

1) точность данных, иначе это приводит к ложным ответам ИИ о человеке;

2) отслеживаемость источников, используемых для дополнения запроса;

3) безопасность данных за счет технических мер разграничения хранения данных;

4) классификация данных по целям их использования, чтобы не использовать данные для нерелевантных целей;

5) чтобы данные привлекались для генерации ответа в объёме необходимом для отработки запроса и не хранились дольше положенного срока;

6) комплаенс по законодательству ещё на этапе обучения языковой модели до имплементации метода RAG;

7) соблюдение всех прав субъектов персональных данных, включая право на доступ к информации об обработке данных.

Организации, использующие ИИ на методе RAG, должны быть готовы доступно объяснить субъектам принципы и условия использования их данных в ИИ-системах.

Практика регулирования защиты персональных данных для ИИ на уровне стандартов может стать популярнее в европейских странах на фоне инициатив по упрощению требований Регламента ЕС по защите персональных данных (GDPR) для целей стимулирования разработчиков ИИ-технологий. В ноябре 2025 г. ожидается презентация Еврокомиссией пакета поправок в GDPR[44]. С учетом того, что европейский подход обращения с персональными данными стал образцом для многих зарубежных национальных законов, ожидается, что новый тренд быстро охватит и другие страны.

Опыт России

В России развиваются стандарты защиты данных для ИИ. Для ИИ в 2022 г. был утвержден ГОСТ по управлению процессами для анализа больших данных (но вопрос защиты персональных данных закрывается отсылкой к общим законодательным требованиям)[45]. В июле 2025 г. Банк России представил Кодекс этики в сфере разработки и применения ИИ на финансовом рынке. В части защиты данных рекомендуется при разработке ИИ-решений использовать данные клиентов только в случаях, если ожидается существенное улучшение эффективности от внедрения ИИ для оказания финансовых услуг[46].

По опросу в 2025 г. в европейских странах, 84% респондентов убеждены, что чем подробнее регулирование вопросов конфиденциальности для ИИ, тем безопаснее его применение[47]. Поэтому в России и мире можно прогнозировать разработку отраслевых стандартов защиты данных для ИИ в таких секторах, как медицинские услуги и электронная коммерция.

[43] Векторными называют базы данных, в которых данные организуются на основе семантического, визуального или иного сходства, что и создает поисковый «вектор» - возможность нахождения примерных ответов на запрос.
[44] https://www.techpolicy.press/eu-set-the-global-standard-on-privacy-and-ai-now-its-pulling-back/
[45] https://docs.cntd.ru/document/1200193996
[46] https://www.cbr.ru/Content/Document/File/178667/code_09072025.pdf
[47] https://employment-social-affairs.ec.europa.eu/news/commission-survey-shows-most-europeans-support-use-artificial-intelligence-workplace-2025-02-13_en