



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

Повторное использование данных в здравоохранении, защита персональных данных при страховании, налогообложение многонациональных компаний, развитие регулирования квантовых технологий

Мониторинг №1(13) (Январь 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.

При частичном или полном использовании материалов ссылка на источник обязательна

«Это январь. Зима
Согласно календарю.
Когда опротивеет тьма,
Тогда я заговорю»

И. Бродский

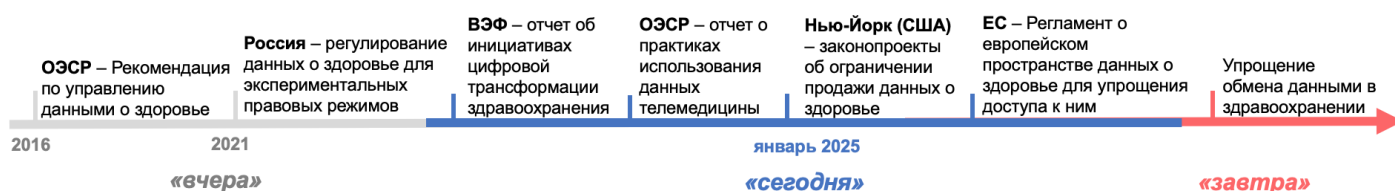
В январе 2025 г. можно выделить 4 события, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Повторное использование данных в здравоохранении

В январе 2025 г. ЕС утвердил Регламент, регулирующий автоматический доступ поставщиков медицинских услуг к данным о здоровье пациента из любой страны ЕС. В Нью-Йорке ужесточается контроль физическими лицами за своими данными о здоровье, например, при использовании медицинских девайсов пользователю должна обеспечиваться возможность удаления данных. ОЭСР выпустила отчет по телемедицине, показав, что сбор данных телемедицины способствует более детальным медицинским исследованиям, а в отчете Всемирного экономического форума (ВЭФ) прогнозируется развитие предиктивного анализа в медицине благодаря доступу к таким данным.

Тренд

Повторное использование данных в здравоохранении



Тренд № 2. Защита персональных данных при страховании

В США проходят судебные разбирательства против страховых компаний о незаконном доступе к данным, а в штате Техас даже инициирован запрет на использование ИИ в страховании для предотвращения необоснованных отказов в покрытии страховых случаев.

Тренд

Защита персональных данных при страховании



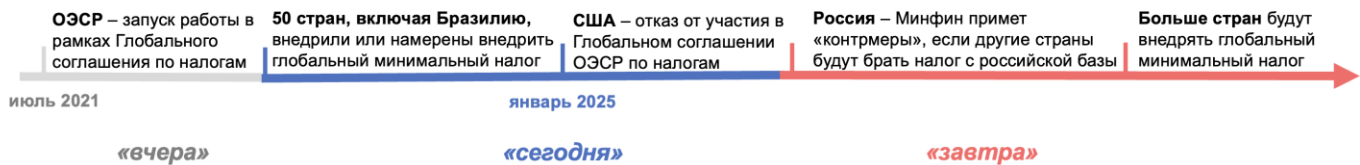
Тренд № 3. Налогообложение многонациональных компаний

В январе 2025 г. США заявили, что не признают права других стран собирать глобальный минимальный налог с американских компаний в рамках Соглашения ОЭСР по налогам¹. Против стран, собирающих такой налог, США введут экономические меры, в том числе сборы в отношении доходов резидентов таких стран, полученных на территории США. Аналогичный подход, возможно, примет Минфин России к середине 2025 г. Бразилия же, наоборот, с января 2025 г. ввела глобальный минимальный налог.

¹ Соглашение – это двухкомпонентный план действий ОЭСР по реформированию международной системы трансграничного налогообложения в рамках борьбы с размыванием налоговых баз и выводом прибылей из-под налогообложения (BEPS).

Тренд

Налогообложение многонациональных компаний



Тренд № 4. Развитие регулирования квантовых технологий

В январе 2025 г. ОЭСР опубликовала Обзор политики в области квантовых технологий, выделив основные риски таких технологий – риски цифровой безопасности и утечки данных, поскольку квантовый компьютер позволяет в разы быстрее, чем классический компьютер, расшифровывать данные и взламывать средства шифрования информации.

Тренд

Развитие регулирования квантовых технологий



В январе 2025 г. в России также произошел ряд значимых событий в сфере регулирования цифровой экономики:

1. Новые правила налогообложения криптовалюты

С января 2025 г. вступают в силу новые правила налогообложения цифровых валют². Можно выделить следующие новации в Налоговом кодексе:

1. Для целей налогообложения криптовалюта признается имуществом по смыслу гражданского законодательства;
2. Майнинг и операции по реализации криптовалют не облагаются НДС;
3. Установлены специальные правила налогообложения майнинга криптовалют.

Для *физических лиц* доходы от майнинга в России признаются доходами от источников в России (не за рубежом), включаются в базу НДФЛ и облагаются по прогрессивной ставке 13-22%. Возможно получить имущественный вычет в размере фактически произведенных и документально подтвержденных расходов майнера, т.е. вычесть расходы, например, на аренду майнингового оборудования, использование электроэнергии и пр.

Важно отметить, что в результате майнинга облагается не доход от продажи криптовалюты, а именно получение самой криптовалюты в натуральной форме (аналогично доходу в виде имущественных прав или товаров и пр.). Возникает вопрос: как подсчитать стоимость полученной намайненной крипты? Стоимость цифровой валюты определяется исходя из ее рыночной котировки на дату ее фактического получения – зачисления криптовалюты на счет майнера, когда у майнера возникает право распоряжаться такой цифровой валютой (например, продать и зачислить цифровую валюту на счет другого лица).

Стоит также отметить, что получение криптовалюты по договору дарения от взаимозависимого лица (например, члена семьи) не облагается НДФЛ.

Для *организаций* доход от майнинга будет облагаться по ставке 25% и будет считаться внереализационным доходом. Как и при НДФЛ, налоговой базой будет считаться рыночная котировка намайненной криптовалюты на дату ее получения, например, в момент зачисления криптовалюты на счет майнера.

² Федеральный закон от 29 ноября 2024 г. № 418-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации». <https://base.garant.ru/411020694/>

Для уплаты НДФЛ и налога на прибыль при майнинге необходимо определить рыночную котировку криптовалюты. Рыночная котировка – это итоговая цена на криптовалюту в конце каждого торгового дня. С учетом того, что деятельность криптобирж в России не урегулирована, то используются рыночные котировки иностранных криптобирж. Такая иностранная криптобиржа должна соответствовать двум условиям: (1) иметь объем торгов криптой более 100 млрд руб. в день и (2) публиковать на сайте информацию о рыночных котировках за последние 3 года.

Если крипто торгуется сразу на нескольких биржах, то налогоплательщик самостоятельно выбирает рыночную котировку на одной из бирж. Если сделки на биржах совершались в иностранной валюте или в других криптовалютах (стоимость должна быть привязана к курсу иностранной валюты), то налогоплательщик вправе выбрать стоимость криптовалюты, пересчитав курс иностранной валюты в рубли по официальному курсу Банка России.

Стоит также отметить, что при майнинге не применяются специальные налоговые режимы, как упрощенная система налогообложения, патентная система налогообложения, налог на профессиональный доход (для самозанятых) и пр.;

4. Установлены специальные правила налогообложения при перепродаже криптовалют.

В результате майнинга налогообложению подлежит сама криптовалюта как доход в «натуральной форме» (описано выше), стоимость которой рассчитывается по рыночным котировкам на иностранных криптобиржах. При этом при дальнейшей перепродаже криптовалюты применяются специальные правила. При перепродаже доход уже будет признаваться «материальной выгодой», поэтому для расчета налога потребуется вычесть разницу стоимости криптовалюты на момент ее зачисления на счет майнера и на момент ее перепродажи третьим лицам. Фактически налогом облагается прирост капитала, произошедший с момента зачисления криптовалюты на счет майнера (или покупателя) и до момента ее перепродажи.

При уплате НДФЛ доход до 2,4 млн руб. от купли-продажи криптовалюты облагается по ставке 13%. При превышении 2,4 млн руб. налог будет рассчитываться по формуле: 312 тыс. руб. + 15% от суммы превышения. Для нерезидентов установлена ставка в размере 30%. При уплате *налога на прибыль организаций* доход определяется исходя из фактической цены продажи криптовалюты, но не ниже рыночной котировки, уменьшенной на 20%. Если лицо понесло убытки при продаже криптовалюты, то можно уменьшить налоговую базу на доходы от криптовалюты в будущем (но не более 50% от суммы убытка) – правило работает как для НДФЛ, так и для налога на прибыль организаций.

Стоит отметить, что в отношении уже имеющихся криптовалют переоценка их стоимости для целей налогообложения производиться не будет;

5. Установлена обязанность оператора майнинг-инфраструктуры каждый квартал направлять в ФНС отчет о лицах, которым он оказывает услуги.

2. Автоматизированное отслеживание Роскомнадзором нарушений оборота персональных данных

Минцифры подготовило проект изменений в Положение о государственном контроле за соблюдением режима обработки персональных данных³. Если ранее нарушения закона о персональных данных выявлялись по обращениям граждан в Роскомнадзор, то теперь Роскомнадзор будет отслеживать такие нарушения «с использованием автоматизированных информационных систем», что позволит мониторить в том числе онлайн-ресурсы. При выявлении нарушения оператору будет направлено уведомление о прекращении незаконной обработки данных в течение 10 рабочих дней. Какие системы будут применяться Роскомнадзором, и каким образом они затронут целостность информационных систем операторов данных, не определено.

³ Постановление Правительства РФ от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» (вместе с «Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных»).

Ключевые аспекты

1. Повторное использование данных в здравоохранении

Опыт ЕС

В январе 2025 г. принят Регламент о Европейском пространстве данных о здоровье (EHDS)⁴. Различаются 2 категории данных о здоровье:

1. Для первичного использования – использование работниками медицинских учреждений данных пациента при оказании услуг;

2. Для вторичного использования – использование данных о здоровье третьими лицами для исследований, статистики и пр.

Для каждой категории Регламент определяет перечни видов данных и правила доступа к ним, а также предусматривает создание двух цифровых платформ для доступа к таким данным: для первой категории – MyHealth@EU, для второй – HealthData@EU.

Регламент наделяет пациентов дополнительными инструментами управления данными, помимо предусмотренных в GDPR⁵:

1) право пациента отказать медицинским организациям в дальнейшем использовании уже собранных медицинских данных. Например, пациент может запросить прекратить хранение данных о результатах его анализов – основания для такого запроса не ограничены;

2) право ограничить цели или условия использования данных. Например, больница может использовать данные только при чрезвычайной необходимости – в случае пандемии;

3) право управлять медицинскими данными – доступ к данным и скачивание в машиночитаемом формате, перенос данных в систему другого поставщика медицинских услуг, право получать уведомления о доступе к их данным и др.

Также предусматривается возможность государств создавать систему «доверенных держателей» данных, которые принимают на себя функции хранения,

обработки данных о здоровье и предоставления их по запросу. Например, если пациент приходит в новый медицинский центр, его данные о здоровье могут быть запрошены от доверенного держателя без необходимости повторного сбора данных у пациента. Цель нового института – устранить дублирование данных в информационных системах больниц и прочих учреждений, путем возложения обязанности на одно лицо хранить данные пациентов для использования разными организациями.

К данным вторичного пользования относятся 17 категорий данных – данные из системы электронных медицинских записей, данные о расходах на медицинские услуги и пр. Устанавливается закрытый перечень целей, для которых может предоставляться доступ к таким данным: статистические исследования, образовательные цели, научные исследования (медицинские, технологические) и пр.

Опыт Нью-Йорка (США)

Предложены 2 законопроекта по регулированию данных о здоровье.

Первый законопроект устанавливает условия обработки данных о здоровье⁶, охватывая в том числе любую финансовую или геолокационную информацию, связанную с физическим или ментальным здоровьем. То есть под защиту подпадают как непосредственно данные о здоровье, так и сведения, связанные с данной сферой жизни лица, например, какие препараты он приобретает, где, как часто и др.

В США по общему правилу действует презумпция, что компании-держатели персональных данных могут продавать данные, если субъект прямо не запретит продавать их. Однако данные о здоровье признаются наиболее чувствительными для пациентов, поэтому законопроект предлагает установить прямой запрет на продажу таких данных. Также предлагается обеспечить пациента правом управления отдельными видами данных, например, давать согласие на обработку данных не в отношении всех данных, а только отдельных,

⁴ <https://digitalpolicyalert.org/event/26173-council-of-the-eu-adopts-regulation-on-european-health-data-space-ehds>

⁵ Общий регламент защиты персональных данных (GDPR) Европейского союза 2016/679.

⁶ <https://digitalpolicyalert.org/event/25961-introduced-new-york-health-information-privacy-act-s-929-to-the-senate>
<https://legiscan.com/NY/text/S00929/id/3040218>

или отзываться согласием в отношении отдельных операций с данными, а не всей обработки данных в целом.

Форма получения согласия может (но необязательно) включать цену обработки данных компанией – такое условие позволяет компенсировать компаниям расходы на обработку данных с учетом запрета коммерциализации данных. Также могут указываться формы компенсации, которые может получить обработчик данных за операции с данными.

Второй законопроект касается конфиденциальности сведений, собираемых электронными медицинскими продуктами, сервисами⁷, девайсами⁸. Законопроект обязывает поставщика устройств, собирающих данные о здоровье пользователей, подробно информировать о судьбе собранных данных. Например, поставщик должен получить разрешение на обмен данными с третьими лицами и информировать пользователя о том, кому именно они будут передаваться. Тем самым законопроект ограничивает неконтролируемое распространение данных о здоровье, собираемых с медицинских устройств (включая их коммерциализацию).

Опыт ОЭСР

ОЭСР выпустила Отчет⁹ по развитию телемедицины. В 2019 г. (до пандемии) на 1 человека в год приходилось в среднем 0,6 телемедицинских консультаций, в 2021 г. – уже 1,4. Анализ данных в здравоохранении показал, что онлайн-консультации не увеличивают нагрузку на отделения первой помощи, а значит рост телемедицины не перегружает систему здравоохранения. В период после пандемии COVID-19 ряд стран приняли меры по развитию медицинских услуг в онлайн и по улучшению управления данными о здоровье. Например, Австралия не только собирает данные по медицинским услугам, оказываемым в рамках системы публичного страхования¹⁰, но также присваивает отличительные идентификаторы для сравнения данных из

различных источников или категорий субъектов. Например, данные коренных народов, данные о лицах, проживающих в пансионатах для пожилых и др. – такие сведения не входят в число данных о здоровье, однако классификация данных по таким критериям необходима для медицинских исследований.

Опыт ВЭФ

ВЭФ представил в отчете о сотрудничестве по данным Инициативу по цифровой трансформации здравоохранения, которая направлена на распространение практик сбора и обмена данными о здоровье и охватывает более 150 организаций¹¹. Участники Инициативы будут обмениваться такими данными, как сведения медицинских карт, поведенческие и социальные показатели, связанные со здоровьем, данные по страховым случаям, данные мониторинга состояния здоровья и др.

Обмен такими данными окажет положительное влияние на инновации и систему здравоохранения. Например, обмен данными повысит выявляемость болезней на ранних этапах (особенно при диагностировании диабета и сердечно-сосудистых заболеваний, на которые приходится 20 млн смертей ежегодно), развивает предиктивный анализ пандемий или заболеваемости, поддерживает распространение превентивной медицины.

Опыт России

В мире наблюдается общая тенденция по формированию правил обращения с данными о здоровье: с одной стороны, в части доступности таких данных для исследований, продажи (как в ЕС), с другой – в части защиты таких данных от несогласованного обращения (как в США). В России повестка по развитию условий обращения с такими данными не обозначена. Как следствие, экономический и инновационный потенциал медицинских данных, собираемых в России, не реализован, например, существуют

⁷ <https://digitalpolicyalert.org/event/25962-introduced-electronic-health-products-and-services-privacy-act-a-1415-to-the-new-york-assembly>
<https://legiscan.com/NY/text/A01415/2025>

⁸ Любое программное обеспечение или программно-аппаратный комплекс, включая приложения, сайты и другие информационные продукты, разработанные для обработки персональных данных о здоровье, в целях предоставления этой

информации пользователю или его поставщику медицинского обслуживания по запросу пользователя.

⁹ https://www.oecd.org/en/publications/leading-practices-for-the-future-of-telemedicine_496a8ffe-en.html

¹⁰ <https://www.aihw.gov.au/about-our-data/our-data-collections/medicare-benefits-schedule-mbs>

¹¹ <https://www.weforum.org/publications/better-together-building-a-global-health-network-economy-through-data-collaboration/>

сложности передачи данных о здоровье для медицинских исследований.

2. Защита персональных данных при страховании

В январе 2025 г. в США инициированы судебные разбирательства против страховой компании Allstate за незаконное получение данных клиентов, а штат Техас предложил запретить использование ИИ для принятия страховыми компаниями решений по медицинской страховке. Стоит отметить, что еще в 2022–2023 гг. ряд страховых компаний столкнулись с крупной утечкой данных: MCNA Dental (США) потеряла данные 9 млн клиентов, Medibank (Австралия) – 9,7 млн¹², Zurich Insurance (Швейцария) – 1 млн.

Опыт США

В январе 2025 г. генеральный прокурор Техаса подал иск против страховых компаний Allstate и Arity (ее дочерней компании) за незаконный сбор, использование и продажу данных о местоположении автопользователей^{13,14}. Allstate покупала у Toyota, Lexus, Mazda, Chrysler, Dodge геолокационные данные с мобильных приложений GasBuddy, Fuel Rewards, Routely¹⁵. Собранные геолокационные данные использовались для корректировки размера страховых премий и покрытия страховых случаев (например, данные наблюдения за водителем в реальном времени позволяют делать выводы о характере вождения и детально рассчитать риски инцидентов)¹⁶. Такая недобросовестная практика затронула права 45 млн пользователей и повлекла для них излишние расходы на страховые услуги.

Также в январе 2025 г. в Техасе был предложен законопроект по регулированию использования технологий ИИ в процедурах оценки пользования пациентами медицинской страховкой^{17,18}. Принятие законопроекта позволит предотвратить

принятие страховыми компаниями автоматизированных решений об отказе в покрытии страховых случаев.

Опыт России

В России страховые компании могут запрашивать медицинские данные для экспертизы у территориальных фондов обязательного медицинского страхования, а в 2022 г. Минздрав подтвердил право страховщиков получать такие данные напрямую от медицинских организаций¹⁹. Но специальные требования к страховщикам по обработке персональных данных российским законодательством не предусматриваются.

3. Налогообложение многонациональных компаний

ОЭСР для борьбы с размыванием налогов многонациональными компаниями (далее – МНК) сформировала «Глобальное соглашение по налогам» (Global Tax Deal), состоящее из двух компонентов. Первый компонент (Pillar 1) предусматривает, что крупные МНК, особенно цифровые, должны уплачивать налоги в странах, где находятся их клиенты, даже если у них нет физического присутствия в этих странах. Второй компонент (Pillar 2) устанавливает глобальную минимальную ставку налога (Global Minimum Tax, GMT) на прибыль организаций в размере 15% для МНК. (В [Мониторинге 10](#) мы описывали работу GMT).

Уже более 50 стран внедрили или планируют внедрить GMT²⁰, с января 2025 г. GMT вводится в Бразилии²¹. Однако в январе 2025 г. США заявили о непризнании GMT для МНК с головными офисами в США.

Опыт США

В январе 2025 г. опубликован Меморандум Президента США о Глобальном налоговом соглашении ОЭСР. Документ направлен против сбора с компаний из США GMT, в частности – против правил сбора в

¹² <https://www.syteca.com/en/blog/data-protection-compliance-insurance-industry>

¹³ <https://digitalpolicyalert.org/event/25955-texas-attorney-generals-issued-fine-following-investigation-into-allstate-and-arity-for-allegedly-unlawful-collection-use-and-sale-of-user-data>

¹⁴ <https://www.malwarebytes.com/blog/news/2025/01/texas-scrutinizes-four-more-car-manufacturers-on-privacy-issues>

¹⁵ <https://natlawreview.com/article/texas-ag-sues-allstate-violations-texas-privacy-law-first-enforcement-action-under>

¹⁶ https://www.theregister.com/2025/01/14/allstate_accused_of_payin_g_app/

¹⁷ Следует пояснить, что в США система медицинского страхования предусматривает процедуры регулярного обзора –

какие медицинские услуги получает пациент на основании страховки в целях формирования индивидуальных планов страхования (health benefits plans).

¹⁸ <https://digitalpolicyalert.org/event/26245-act-relating-to-use-of-artificial-intelligence-in-utilization-review-conducted-for-health-benefit-plans-sb-815-was-introduced-to-the-senate>

¹⁹ <https://medvestnik.ru/content/news/Minzdrav-podtverdil-obyazannost-meduchrejdennii-predostavlyat-SMO-originaly-dokumentov.html>

²⁰ <https://www.pwc.com/gx/en/tax/international-tax-planning/pillar-two/pwc-pillar-two-country-tracker-summary-v2.pdf>

²¹ <https://legislacao.presidencia.gov.br/atos?tipo=LEI&numero=15079&ano=2024&ato=452EzaE1UNZpWta29>

отношении недообложенных налогом доходов МНК²². Это правило позволяет странам взимать дополнительный налог с международных (в частности, американских) компаний, если их налоговая ставка в другой стране ниже 15% (размер GMT). Таким образом компенсируются недостающие налоговые поступления, если страна, где получен доход, не доводит налог до уровня 15%, предложенного ОЭСР.

В развитие Меморандума был представлен законопроект «О защите американских рабочих мест и инвестиций»²³, направленный против экстерриториальных налогов, которые иностранные государства вводят в отношении граждан и компаний США (в том числе против стран, вводящих GMT). Минфин США должен регулярно составлять отчеты о таких налогах, а затем добиваться их отмены через двусторонние переговоры. Если страна не устранил такие налоги, могут вводиться ответные меры, включая повышение налогов для граждан и компаний этой страны, а также ограничения в сфере торговли.

Опыт Бразилии

В Бразилии с 1 января 2025 г. применяется GMT ОЭСР в виде дополнительного сбора к социальному налогу на чистую прибыль²⁴ для МНК с доходом свыше 750 млн евро. Если ранее ставка составляла 9%, теперь иностранные МНК будут платить в Бразилии еще 6% с дохода в Бразилии, чтобы достичь минимальной ставки GMT в 15%.

Опыт России

Еще в декабре 2024 г. Минфин России опубликовал заявление, что в середине 2025 г. будет принято решение «о необходимости донастройки национального законодательства» в связи с Pillar 2, и если «в 2024 году компания заплатила налог с российской налоговой базы не в России», то

будут приняты «контрмеры»²⁵. Заявление позволяет сделать вывод, что Минфин России в вопросах реализации Pillar 2 может последовать подходу, аналогичному США: невнедрение GMT и непризнание прав других стран на его взимание с российских компаний.

4. Развитие регулирования квантовых технологий

Опыт ОЭСР

В январе 2025 г. ОЭСР опубликовала Обзор политики в области квантовых технологий²⁶. Квантовые технологии – технологии, использующие квантовые эффекты (уникальное поведение очень маленьких частиц на атомном и субатомном уровнях) для сбора, обработки и передачи информации, включая квантовые сенсоры²⁷, квантовые вычисления²⁸, квантовые коммуникации²⁹.

ОЭСР выделяет ряд преимуществ квантов. Например, квантовые сенсоры (как атомные часы) могут способствовать точной синхронизации времени (до микросекунд) в высокочастотной торговле на фондовых биржах, позволяя определять оптимальный момент времени покупки и продажи активов на торгах. Квантовый генератор случайных чисел генерирует безопасные пароли для онлайн-транзакций. Квантовая коммуникация за счет кодирования повышает безопасность центров обработки данных при хранении данных³⁰. Так, в Лондоне компании BT и Toshiba в 2021 г. запустили сеть передачи данных с квантовой защитой для безопасности финансовых операций (присоединился банк HSBC³¹). Мощные вычислительные возможности квантовых компьютеров могут снижать издержки на дорожающее обучение все новых моделей ИИ – стоимость обучения модели OpenAI для первой версии ChatGPT GPT-3 оценивалась

²² Undertaxed Profits Rule

²³ <https://gop-waysandmeans.house.gov/wp-content/uploads/2023/05/Defending-American-Jobs-and-Investment.pdf>

²⁴ Social Contribution on Net Income, часть налога на прибыль организаций в Бразилии.

²⁵ https://minfin.gov.ru/ru/press-center/?id_4=39517-aleksei_sazanov_zakonoproekt_o_prodlennii_nulevoi_stavki_nds_dlya_gostinitits_budet_podgotovlen_v_pervoi_polovine_2025_goda

²⁶ https://www.oecd.org/en/publications/a-quantum-technologies-policy-primer_fd1153c3-en.html

²⁷ Измеряет физические величины, такие как масса, время и интенсивность света, например, атомные часы, фотонные детекторы.

²⁸ Предназначается для работы с данными; их скорость решения задач намного быстрее классического компьютера.

²⁹ Использует квантовые свойства частиц для кодирования и передачи информации, например, квантовое распределение ключей - шифрует криптографические ключи в кубитах (квантовая криптография).

³⁰ Например, использовалась для безопасной передачи данных между ЦОД Siemens в Нидерландах в 2010 г.

³¹ <https://www.toshiba.eu/solutions/quantum/news/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network/>

в 4,6 млн долл., а для версии GPT-4 – более чем в 100 млн долл.

ОЭСР выделяет риски развития квантов:

1. Угроза безопасности данных в интернете. Квантовый компьютер может быстрее расшифровывать данные. Так, взломать RSA-2048 (криптографический алгоритм для защиты данных) самый быстрый суперкомпьютер может за 300 трлн лет, квантовый компьютер – за несколько часов. Поэтому Национальный центр кибербезопасности Великобритании рекомендует компаниям уже сегодня внедрять квантово-устойчивые решения – специальные методы по защите данных от квантовых компьютеров, поскольку существуют риски, что хакеры могут похитить зашифрованные данные сейчас и хранить их до появления квантовых компьютеров для расшифровки данных в будущем.

2. Риски конфиденциальности. Так, квантовые сенсоры могут вести слежку за людьми (видеть сквозь одежду, здания, материалы), перехватывать сигналы связи устройств, находящихся на близком расстоянии (что позволяет получать информацию с банковских карт и смартфонов). Использование квантовых сенсоров в медицине поднимает вопрос защиты персональных данных: требуется получить «информированное согласие» от пациента на сбор и использование данных – пациент может не понимать, какая информация собирается высокочувствительными квантовыми сенсорами.

Для развития квантовых технологий ОЭСР предлагает разрабатывать контрольные показатели (метрики, бенчмарки) для оценки и сравнения возможностей таких технологий (например, частота ошибок в вычислениях, точность вычислений, скорость генерации кода, чувствительность сенсоров); развивать международные стандарты для развития технологии. Например, уже выпущены стандарты Международной организации по стандартизации (ISO) (словарь ISO/IEC 4879:2024 по квантовым вычислениям), Международной электротехнической комиссии (IEC), стандарты Европейского института телекоммуникационных

стандартов (ETSI) («Квантовое распределение ключей» (QKD)) и пр.

Опыт России

В России в 2023 г. принята Концепция регулирования отрасли квантовых коммуникаций (до 2030 г.), направленная на создание единых национальных технических требований к квантовым сетям, поставщикам такого оборудования. Приняты стандарты, закрепляющие основные термины (ПНСТ 830-2023), стандарты криптографической защиты информации (ПНСТ 799-2022) и другие. Однако в России не решена проблема оценки рисков безопасности и уязвимостей перед квантовыми угрозами на уровне государственных и общественных информационных систем и каналов связи (например, банковских или с помощью технологии блокчейн) и пр.