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

- **ИИ в критических сферах**
- **Защита детей в Интернете**
- **Антиконкурентные практики онлайн**
- **Доступ к банковским данным**
- **Цифровизация здравоохранения**
- **Упрощение условий работы с данными**

Мониторинг №11 (23) (Ноябрь 2025)

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

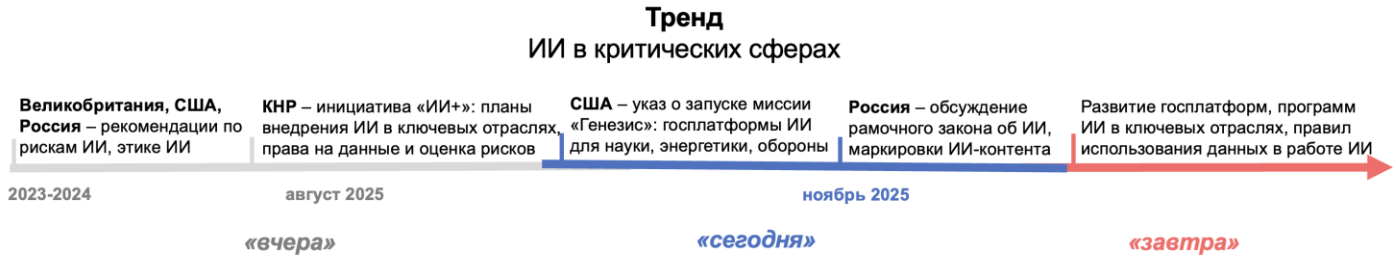
Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Магомедова О.С., науч. сотр. Черновол К.А., науч. сотр. Фонда Экономической политики Голованова Д.А.

«Простишь ли мне эти ноябрьские дни?
В каналах приневских дрожат огни.
Трагической осени скудны убранства.»
А. Ахматова

В ноябре 2025 г. можно выделить 6 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

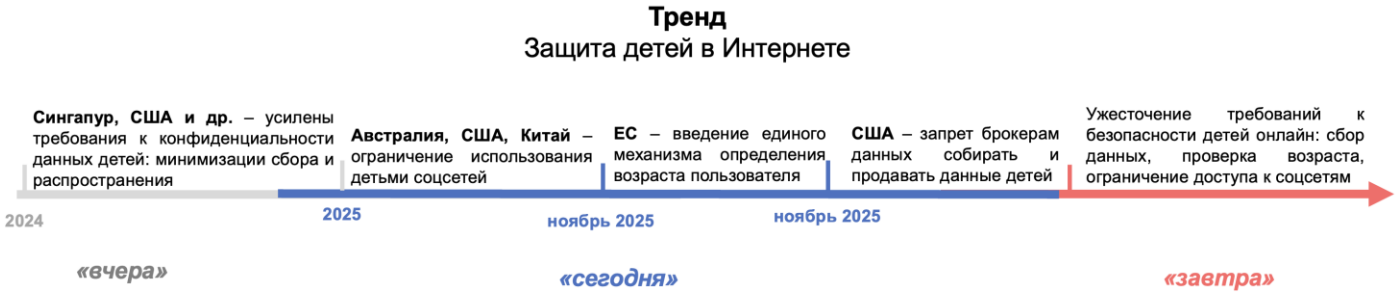
Тренд № 1. ИИ в критических сферах

В ноябре 2025 г. в США запланирован запуск государственной ИИ-платформы для науки, энергетики и обороны с доступом компаний к данным и вычислительным мощностям.



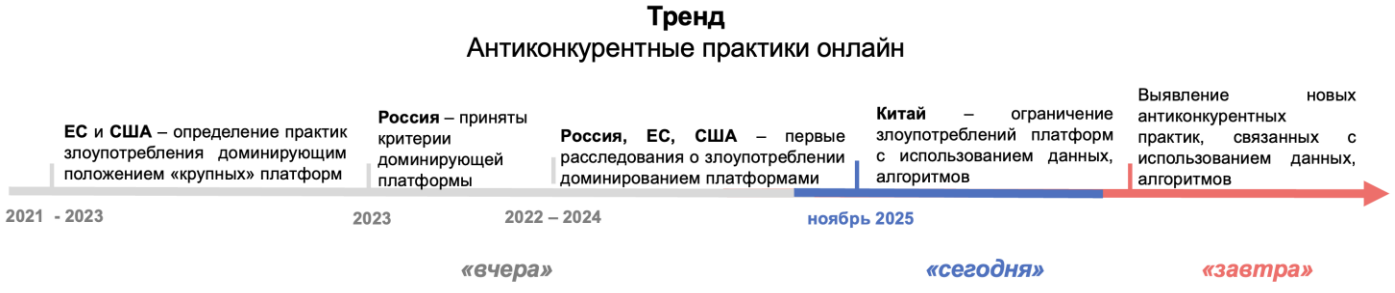
Тренд № 2. Защита детей в Интернете

В ноябре 2025 г. ЕС принял Резолюцию об усилении защиты детей в Интернете, включая контроль за детскими «инфлюенсерами». В США предложено запретить собирать, хранить и продавать персональные данные несовершеннолетних брокерами данных.



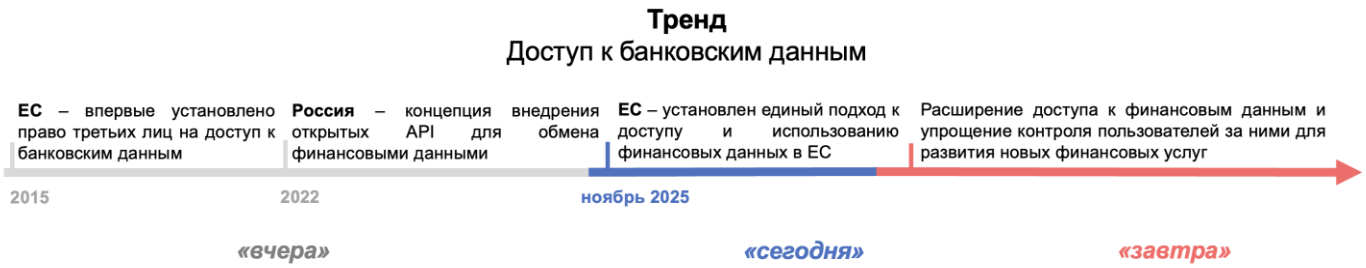
Тренд № 3. Антиконкурентные практики онлайн

В ноябре 2025 г. в Китае опубликовано Руководство по антимонопольным практикам платформ, таким как сговор путем обмена чувствительными данными, злоупотребление доминированием через использование алгоритмов и пр.



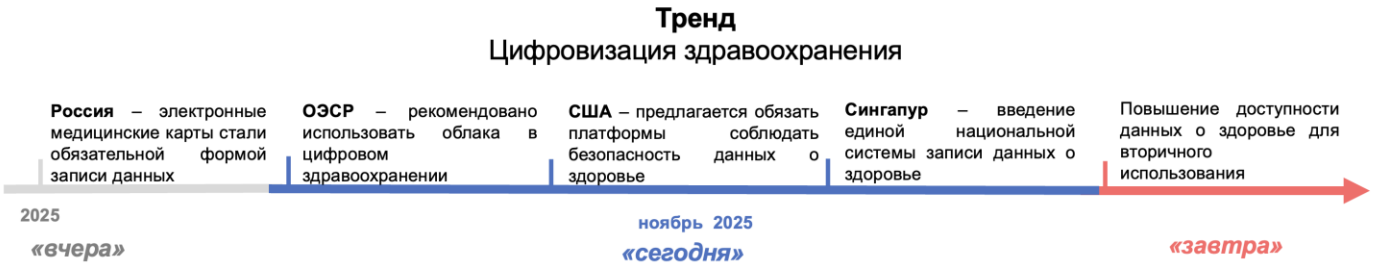
Тренд № 4. Доступ к банковским данным

В ноябре 2025 г. в ЕС была согласована новая Директива о платёжных услугах, устанавливающая правила доступа лицензированных провайдеров открытого банкинга к данным счетов пользователей.



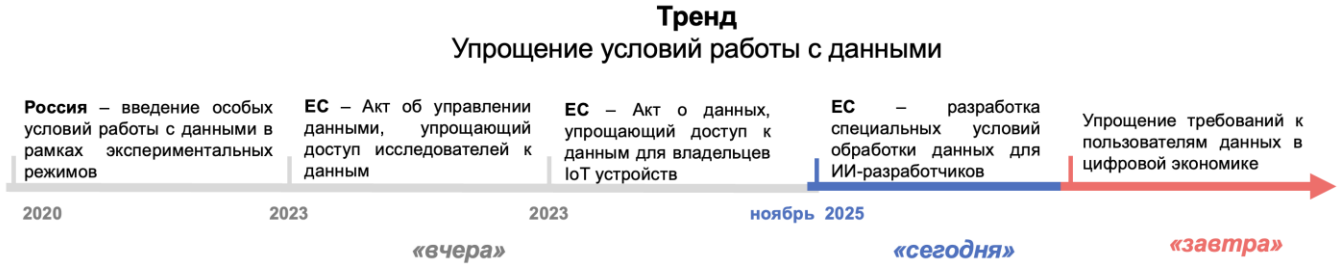
Тренд № 5. Цифровизация здравоохранения

В ноябре 2025 г. ОЭСР представила доклад по лучшим практикам стран по цифровизации публичного здравоохранения. В США, например, предложено возложить на поставщиков цифровых сервисов обязательства по защите данных о здоровье, которые раньше распространялись только на больницы и страховщиков.



Тренд № 6. Упрощение условий работы с данными

В ноябре 2025 г. ЕС представил пакет поправок в целях упрощения требований по обращению с данными.



Также в России в ноябре 2025 г. Роскомнадзор приступил к поэтапной **блокировке WhatsApp**[1] из-за отказа сервиса предоставлять информацию по запросам российских регуляторов, включая сведения об утечках данных и использования мессенджера для мошенничеств и другой преступной деятельности[2] –- формальное нарушение ст.10.1 Закона об информации, требующее от мессенджеров сотрудничать с государственными органами.

[1] Принадлежит компании Meta. Деятельность компании Meta признана экстремистской и запрещена на территории Российской Федерации.
[2] Из официального заявления РКН для ТАСС. https://tass.ru/ekonomika/25764077

Ключевые аспекты

1. ИИ в критических сферах

Опыт США

С ноября 2025 г. в США запущена миссия Genesis[3] по созданию «Американской платформы науки и безопасности» для научных данных в целях обучения фундаментальных моделей и «агентов ИИ», которые проверяют гипотезы и автоматизируют исследования в приоритетных сферах: энергетика, научные исследования и разработки, оборона. Платформа разработана в развитие «Плана Америки по ИИ»[4] (см. обзор в Мониторинге №7 (19) (Июль 2025)).

Платформа должна обеспечить вычислительные мощности, средства моделирования и анализа, защищённый доступ к данным и пр. Планируется развивать ИИ в сфере передовых производств[5], биотехнологий, критических материалов, ядерной энергетики, квантовых вычислений, полупроводников и микроэлектроники.

Предполагается разработка типовых соглашений по данным и моделям, правил лицензирования и коммерциализации результатов интеллектуальной деятельности, созданных с использованием платформы, а также единых процедур доступа к данным, моделям и вычислениям, стандарты кибербезопасности для негосударственных участников.

В настоящее время в миссии Genesis планируется участие 53 компаний в сфере облачных технологий и платформ ИИ общего назначения (5 компаний), аппаратного обеспечения и инфраструктуры дата-центров для ИИ (10), полупроводников, литографии и критических материалов для ИИ-инфраструктуры (12), энергетики, в том числе ядерной (6), квантовых вычислений (2) и др. Инициатива Genesis – это вовлечение бизнеса в разработки ИИ-решений, в том числе за счет бюджетных средств. Планируется подключение стартапов.

Опыт Китая

В августе 2025 г. опубликованы Мнения об углублении реализации инициативы «Искусственный интеллект+» о формировании программ, стандартов, правовом регулировании ИИ. Документ содержит направления:

– для науки и технологий – развитие научных моделей и создание открытых и совместно используемых высококачественных наборов научных данных;

– внедрение ИИ в стратегии и процессы предприятий и применение ИИ при проектировании, производстве и обслуживании;

– улучшение системы прав на данные и авторских прав применительно к ИИ, открытие доступа к данным, созданным в рамках проектов с государственным финансированием, параллельно - развитие национальной вычислительной инфраструктуры (чипы для ИИ, сверхкрупные вычислительные кластеры и пр.);

– создание правил мониторинга работы систем ИИ, предупреждения рисков и реагирования на инциденты с учетом уровня риска. Здесь подход КНР к регулированию ИИ схож с подходом ЕС.

В отличие от США, подход Китая не строится вокруг одной конкретной государственной платформы с жёстким режимом допуска партнёров[6]. Вместо этого Китай внедряет ИИ «во всех секторах» экономики и управления и параллельно планирует «донастроить» рамочные правила: права на данные и авторские права, стандарты, систему оценки безопасности и регистрационного учёта, а также мониторинг и реагирование на риски ИИ.

Опыт России

В ноябре 2025 г. Минцифры России обсуждало запуск пилотного проекта по маркировке контента, созданного ИИ, что позволит различать контент, созданный человеком и машиной, а также механизмы подтверждения личности пользователей, размещающих материалы. Было предложено

[3] https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/

[4] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

[5] Производство с использованием ИИ, Интернета вещей, 3D-печати и т.п.

[6] Типовые соглашения по данным и моделям, единые процедуры доступа, требования к кибербезопасности, проверка и авторизация пользователей.

проанализировать действующее регулирование ИИ, оценить насколько существующие нормы защищают права граждан при использовании ИИ в здравоохранении, образовании и социальной поддержке, и где остаются пробелы – еще раз рассмотреть основные нормы закона об ИИ[7].

В перспективе в мире и России будут разрабатываться законы об ИИ, определяющие принципы использования технологии и распределения ответственности за корректную работу систем ИИ в критически важных сферах (в социальной сфере, здравоохранении и пр.) между государством, разработчиками и поставщиками цифровых услуг. В среднем в развитых странах в ближайшие годы около 15% всех проектов в сфере ИИ будут финансироваться государствами, сегодня разброс такой доли составляет от 3% (США[8]) до около 50% (КНР[9]).

2. Защита детей в Интернете

Опыт ЕС

В ноябре 2025 г. ЕС принял резолюцию[10] об усилении защиты детей в Интернете из-за чувствительности к деструктивному контенту, созданному ИИ, игровой зависимости, психическим расстройствам из-за социального давления в Интернете и пр. Еще в октябре 2025 г. Еврокомиссия начала расследования[11] нарушений Snapchat, YouTube, App Store и Google Play по защите[12] несовершеннолетних в части наличия механизмов проверки возраста, установления по умолчанию более строгих настроек конфиденциальности учетных записей, обеспечения дизайна сервиса, не вызывающего зависимость и пр.

ЕС планирует разработать:

1) единый способ проверки возраста пользователя на пространстве ЕС. Способ должен обеспечивать минимальный сбор данных детей, например, получение только утвердительного или отрицательного ответа на вопрос, достиг ли пользователь 16 лет[13], чтобы пользоваться платформой, без сбора данных для идентификации лица;

2) требования к производителям устройств, приложений ИИ к механизму контроля за сбором данных, чтобы приложения ИИ не собирали данные ребенка без согласия родителя, опекуна;

3) запрет платформам финансово поддерживать «детских инфлюенсеров» (например, оплачивать размещение рекламы), создание способа разграничения контента и рекламы в приложениях для детей;

4) требование к платформам запрещать размещать игры, в которых есть «лотерейные» механизмы (как «колеса фортуны», механизмы «плати, чтобы продвигаться в игре», обмен игровой валюты на реальные деньги и пр.);

5) требование к платформе, приложению на этапе разработки создать инструменты родительского контроля (например, получение родителем отчета о действиях ребенка на платформе).

Опыт США

В ноябре 2025 г. представлен законопроект[14] о запрете брокерам данных[15] собирать, использовать, хранить, а также распространять (продавать, раскрывать) данные несовершеннолетнего[16]. Единственное исключение – сбор данных брокером для определения возраста человека. Требуется удалять любые данные лица после установления возраста и создать механизм подачи запроса на удаление данных ребенка (например, родителем, опекуном, самим подростком).

Опыт России

В России Закон № 436-ФЗ «О защите детей от информации, причиняющей вред их

[7] https://www.youtube.com/watch?v=pekDcfdiNhI
[8] https://www.nitrd.gov/pubs/FY2025-NITRD-NAIIO-Supplement.pdf
[9] https://techwireasia.com/2025/06/china-ai-investment-98-billion-2025-us-rivalry
[10] https://www.europarl.europa.eu/doceo/document/TA-10-2025-0299_EN.pdf
[11] https://ec.europa.eu/commission/presscorner/detail/en/mex_25_2353
[12] Проверки соответствия требованиям Закона о цифровых услугах ЕС 2022 г.
[13] 16 лет признается Парламентом как возраст, когда подросток может самостоятельно без контроля со стороны родителя использовать соц. сеть
[14] https://www.congress.gov/bill/119th-congress/house-bill/6292/text
[15] Брокер данных - юридическое лицо, которое продает, сдает в аренду, торгует, передает, раскрывает или иным образом предоставляет третьим лицам полученные персональные данные физического лица, но которые эта организация не собирала непосредственно от такого физического лица.
[16] Законопроект разграничивает категории возраста несовершеннолетнего: ребенок (до 13 лет); подросток (от 13 до 18 лет). Подросток может подать запрос на удаление своих ПД, а ребенок самостоятельно без родителя/опекуна – нет.

здоровью и развитию» устанавливает возрастную квалификацию для ограничения деструктивного контента, определяет обязанность платформы, операторов связи ограничивать доступ к контенту. Тренд на меры защиты детей будет расширяться, особенно с развитием доступа к новым технологиям. Так, прогнозируется, что только применение ИИ в образовании детей будет расти на 38,5% в год до 2030 г.[17].

3. Антиконкурентные практики онлайн

Опыт Китая

В ноябре 2025 г. в Китае выпущено Антимонопольное руководство для платформ[18]. Платформы обязаны внедрить систему комплаенса, управлять рисками.

Установлены следующие правила:

1. Запрет горизонтальных соглашений (между платформами или пользователями платформ) о фиксировании цен, ограничении объемов продаж, ограничении внедрения новых технологий или продуктов путем:

– формирования общих пулов данных, соглашений об интероперабельности между системами, использования облачных хранилищ, ИИ для согласования намерений обмена информацией;

– обмена чувствительной информацией (о ценообразовании, комиссиях, условиях скидок, клиентских базах, механизмах распределения трафика и пр.);

– использования данных, алгоритмов, правил платформы для согласованного единообразного поведения для сегментации пользователей, динамического ценообразования, распределения трафика, ранжирования товаров.

2. Запрет вертикальных соглашений (между платформой и продавцами) об установлении перепродажных цен, используя:

– анализ больших данных, ИИ и других средств для автоматической установки цен;

– профили пользователей, прогнозные алгоритмы и пр. для прямого или косвенного ограничения перепродажных цен.

Платформа не должна способствовать заключению таких соглашений между участниками платформы.

3. Запрет злоупотребления доминирующим положением через практики:

– несправедливо высоких сборов, комиссий за обслуживание, маркетинг;

– скрытое завышение цен (дробление сервисных пакетов, дополнительные виды платных услуг);

– несправедливо низкие закупочные цены (выплата продавцам цен за товары, которые явно ниже цен, выплачиваемых другими платформами);

– продажи по цене ниже себестоимости (например, субсидирование цен продавцов) для ограничения конкуренции (после вытеснения конкурентов с рынка резкое повышение цены);

– отказ от сделок с контрагентами, ограничивая конкуренцию: снятие товаров с продажи, блокировка аккаунтов, установление чрезмерно сложных процедур совершения сделок, ограничение трафика, прекращение обмена данными, в том числе. с использованием алгоритмов распределения трафика, размещения товаров и пр.;

– ограничение сделок, например, включение в правила платформы требований к продавцам не работать с другими платформами, в том числе под угрозой исключения из акций, программ лояльности, блокировки, понижения позиций в результатах поиска, ограничения трафика, создания технических препятствий и пр.;

– требование приобретать определенные товары (связанные продажи) и навязывание необоснованных условий сделки, например, использование всплывающих окон, обязательных для прохождения шагов в интерфейсе, возложение на продавцов расходов за участие в промоакциях платформы, ограничения способов совершения сделок, оплаты, взимание необоснованных платежей (технические сборы, плата за продвижение в трафике и др., о которых не было известно заранее);

– дискриминация пользователей платформы – разные правила подключения к

[17] https://www.applify.co/insights/gen-ai-for-k12

[18] https://www.samr.gov.cn/hd/zjdc/art/2025/art_8e05960782204036af6b9583f1413378.html

платформе, взимания платежей как для продавцов, так и для покупателей (например, на основе данных о предпочтениях, истории сделок, используемых устройствах, анализе платежеспособности и пр.).

Платформы обязаны внедрить систему антимонопольного комплаенса, проводить последующее управление рисками (например, специальную оценку после проведения маркетинговых кампаний, инвестиционных сделок и пр.).

Опыт России

В России с октября 2026 г. вступит в силу Закон о платформенной экономике, который регулирует отдельные антиконкурентные практики платформ, например, запрет для маркетплейсов принуждать продавцов к участию в распродажах, равный доступ для всех продавцов к возможностям услуг (продвижения в поисковой выдаче и пр). Однако законодательство о конкуренции пока не содержит специальный перечень практик, характерных для онлайн-рынков, например, злоупотребление доминирующим положением за счет различных технологий, таких как замедление трафика браузеров, ограничение работы прогрессивных приложений, манипулирование формами согласия на сбор данных и пр.

Наблюдается усиление внимания органов к антиконкурентному поведению платформ: среднегодовое число антимонопольных дел в цифровых секторах выросло с 4 дел в год в 2015 г. до 29 дел в год в 2015–2022 гг.[19]

4. Доступ к банковским данным

Опыт ЕС

В ноябре 2025 г. в ЕС согласована новая Директива о платёжных услугах (PSD3)[20], регулирующая деятельность поставщиков платёжных услуг (банки и небанковские финтех-компании) и порядок доступа к данным платёжных счетов пользователей в рамках открытого банкинга[21].

При наличии согласия пользователя провайдеры открытого банкинга (сервисы, которым он разрешает получать данные счёта или проводить платежи) должны иметь доступ к данным его платёжного счёта, а банки обязаны предоставлять такой доступ на недискриминационной основе (предоставлять его всем лицензированным провайдерам на одинаковых условиях).

У пользователя появляется больше контроля над доступом к своим данным: предусматривается создание панели управления разрешениями, с помощью которой пользователи платёжных услуг смогут в одном месте видеть, каким провайдерам они предоставили доступ к данным своих платёжных счетов, и управлять выданными согласиями.

Дополнительно, PSD3 затрагивает техническую сторону платёжных услуг: мобильные устройства и цифровые сервисы не должны создавать технические ограничения для работы платёжных приложений. Производители смартфонов (управляющие устройством и его операционной системой) и поставщики электронных услуг (сервисы, обеспечивающие доступ приложений к функциям устройства) будут обязаны обеспечивать возможность хранения и передачи данных, необходимых для проведения платежей, со стороны таких приложений.

Опыт России

В России аналогичный механизм открытого доступа к банковским данным пока находится в стадии разработки. Ещё в 2022 г. Банк России представил концепцию внедрения открытых API[22] (инструментов для безопасного обмена данными между банками и другими финансовыми компаниями) на финансовом рынке, а в 2024 г. опубликовал план, предполагавший обязательное подключение API для крупнейших банков с 2026 г. (а для остальных участников с 2027)[23]. Пока крупнейшие банки обмениваются данными через API в рамках отдельных партнёрств. До конца 2025 г. ЦБ

[19] https://www.cresse.info/wp-content/uploads/2024/09/2024_ps20_pa3_POIRIER_GARNEAU.pdf

[20] https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2023/0209(COD)

[21] Механизм, при котором пользователи могут передавать данные о своих платёжных счетах лицензированным финансовым компаниям через стандартизированные интерфейсы.

[22] Программные интерфейсы, которые позволяют финансовым организациям безопасно передавать данные внешним участникам.

[23] https://www.cbr.ru/Content/Document/File/142114/concept_09-11-2022.pdf

РФ планирует подготовить и опубликовать проекты единых стандартов информационного обмена для открытых API.

По прогнозам, доступ к финансовым данным будет продолжать расширяться: к 2030 г. мировой рынок открытого банкинга вырастет с 31 млрд долл. в 2024 г. до 135 млрд долл.[24]

5. Цифровизация здравоохранения

Опыт стран ОЭСР

В ноябре 2025 г. ОЭСР представила доклад по цифровизации публичного общественного здравоохранения[25], выделив лучшие практики в 4 направлениях:

1. Наращивание кадрового потенциала. В Австралии запущена программа по повышению цифровой грамотности медицинских специалистов, где врачи обучаются работе с медицинскими информационными системами больниц;

2. Технологическое оснащение. ОЭСР рекомендует для хранения данных в здравоохранении использовать облачные решения (снижение нагрузки на ИТ-инфраструктуру больниц); установить критерии обеспечения конфиденциальности данных в процедурах госзакупок ПО для больниц; обеспечивать масштабируемость ИТ-решений для больниц; использовать открытое ПО со встроенными стандартами совместимости для взаимодействия больниц;

3. Формирование архитектуры данных о здоровье. В Новой Зеландии утверждены стандарты интероперабельности данных и информационных систем для обмена между больницами наиболее часто запрашиваемых данных о здоровье;

4. Организация участия населения в управлении данными. В Канаде принят стандарт самоуправления данными о здоровье для коренных народов, которые могут самостоятельно регулировать сбор и доступ к данным в медицинских организациях.

Опыт США

В ноябре 2025 г. в США предложена реформа защиты конфиденциальности медицинской информации[26]: рекомендовано возложить на поставщиков цифровых сервисов для медицинских услуг (аналог СберЗдоровья, SmartMed и др.) обязательства, аналогичные обязательствам операторов данных. Эти обязательства установлены Законом о переносимости и подотчетности медицинского страхования (HIPAA) только в отношении больниц и страховых компаний. Такие организации, как платформы, не несут обязательств по защите данных о здоровье.

Закрепляются и права субъекта персональных данных на доступ к данным, удаление и перенос данных, на отказ от продажи его данных третьим лицам, на получение уведомлений, изложенных ясным языком в понятной форме – ранее такие права закреплялись на уровне штатов, теперь на федеральном уровне.

Опыт Сингапура

В Сингапуре продолжается[27] создание национальной системы электронных записей для сбора, хранения и раскрытия данных о здоровье. Больницы обязаны загружать в систему конкретные виды данных пациентов и соблюдать технические требования. Доступ к информации в системе получат сами субъекты данных и поставщики медицинских услуг, включая аптеки. В системе можно получить доступ к 2 типам данных:

1) прямо идентифицирующая физическое лицо информация о здоровье (используется для оказания медицинских услуг пациентам);

2) обезличенные и агрегированные данные из больниц для исследователей. Для получения данных исследователи должны указать цель запроса информации и намерения по дальнейшему раскрытию полученной информации третьим лицам.

Опыт России

В России еще в 2024 г. было утверждено «Стратегическое направление в области цифровой трансформации здравоохранения до 2030 года», включая формирование доступа пациентов и

[24] https://www.grandviewresearch.com/industry-analysis/open-banking-systems-market

[25] https://www.oecd.org/en/publications/digitalisation-of-public-health_97204768-en.html

[26] https://www.congress.gov/bill/119th-congress/senate-bill/3097/text?s=1&r=6

[27] https://www.parliament.gov.sg/docs/default-source/bills-introduced/health-information-bill-20-2025980b6831-a710-4386-bb27-f7b7f53d1f95.pdf?sfvrsn=95b05d08_1

медицинских организаций к данным о здоровье через ЕГИСЗ[28]. С 2025 г. ведение медицинских записей в электронном формате стало обязательным для всех медицинских организаций. Однако экономический потенциал такого сбора данных о здоровье не реализуется полностью – к собранным данным не предусмотрен централизованный доступ для исследователей или для разработчиков медицинских технологий. Открытие доступа к таким данным позволит снизить до 9% расходы на проведение исследований за счет снижения доли дублирований в исследованиях[29].

6. Упрощение условий работы с данными

Опыт ЕС

В ноябре 2025 г. Еврокомиссия представила пакет поправок в акты ЕС по упрощению управления данными для поддержки инноваций, особенно ИИ[30]. Инициатива включает адаптацию Общего регламента по защите данных (GDPR) под нужды разработчиков ИИ-систем:

1) предлагается ввести отдельное основание законной обработки персональных данных для целей разработки и тестирования ИИ-систем и ИИ-моделей: разработчикам больше не нужно получать отдельное согласие на обработку данных для целей обучения ИИ, чтобы обезличить эти данные и включить в базу данных для обучения ИИ;

2) предлагается решение проблемы ре-идентификации обезличенных данных в процессе их анализа с помощью ИИ. Если раньше это приводило к необходимости принять меры по удалению ре-идентифицированных данных из баз данных, то теперь разработчикам ИИ достаточно принять меры по предупреждению раскрытия восстановленных персональных данных третьим лицам. Важно не допускать, чтобы языковая модель выдавала ответ на запрос с демонстрацией персональных данных.

Опыт России

В России задача упрощения доступа к данным для участников цифровой экономики, например, разработчиков новых технологий, решается на уровне экспериментально-правовых режимов (ЭПР). Механизм ЭПР применяется с 2020 г., и предполагает разработку специальных условий доступа и работы с данными в рамках каждого запускаемого ЭПР. Однако ЭПР действует ограниченно по кругу участников, поэтому упрощение условий доступа к персональным данным в рамках одного ЭПР не позволяет стимулировать развитие технологий, основанных на данных, по всей стране. В России и в мире будут развиваться новые режимы централизованного доступа к данным с более широким кругом участников разных отраслей экономики. Сегодня в таком формате уже организуется европейское пространство данных в отдельных секторах, таких как здравоохранение.

[28] Единую государственную информационную систему в сфере здравоохранения.

[29] https://handbook.pathos-project.eu/sections/0_causality/open_data_cost_savings.html

[30] https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal