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

Ограничение работы DeepSeek, обязанность платформ выплачивать чаевые, ограничение продажи персональных данных, защита интеллектуальных прав при обучении ИИ, антиконкурентные практики онлайн

Мониторинг №2 (14) (Февраль 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.

«Февраль. Достать чернил и плакать!
Писать о феврале навзрыд,
Пока грохочущая слякоть
Весною черною горит»
Б. Пастернак

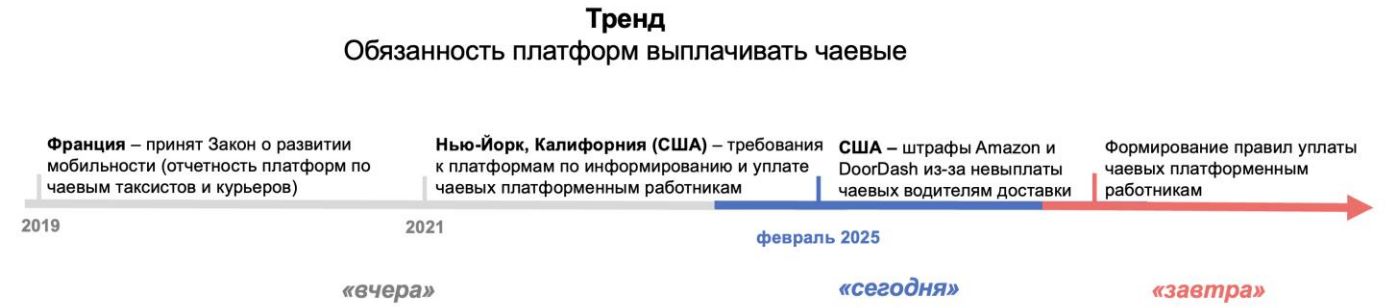
В феврале 2025 г. можно выделить 5 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Ограничение работы DeepSeek

В феврале 2025 г. ряд стран (ЕС, США, Австралия) ввели меры по ограничению или запрету использования приложения DeepSeek (Китай). Это чат-бот, аналогичный OpenAI ChatGPT. Главные причины введения запретительных мер – угрозы цифровой безопасности и неправомерное использование персональных и иных данных.

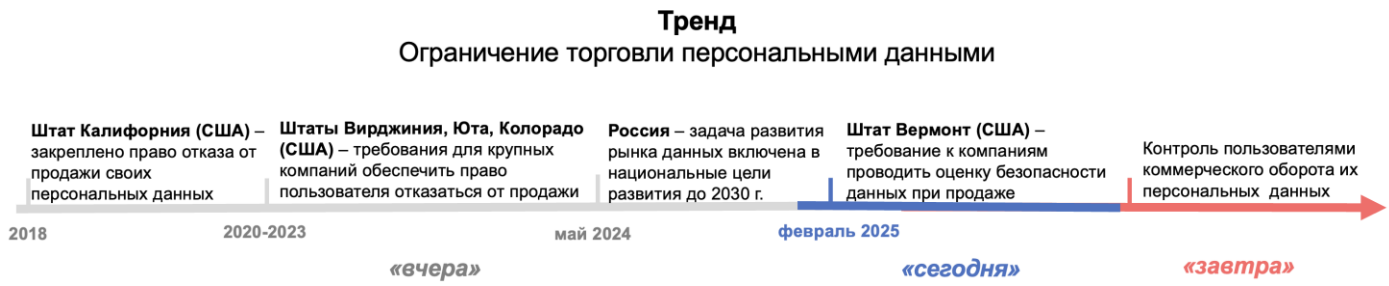
Тренд № 2. Обязанность платформ выплачивать чаевые

В феврале 2025 г. в США назначены штрафы Amazon и DoorDash в связи с невыплатой чаевых своим водителям доставки.



Тренд № 3. Ограничение продажи персональных данных

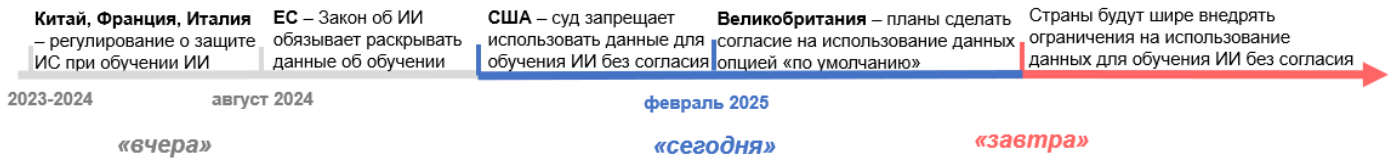
В феврале 2025 г. в штате Вермонт (США) представлен законопроект, обязывающий крупные компании, продающие персональные данные, обеспечивать лиц инструментами контроля продажи их данных. В США формируется тренд на ограничение неконтролируемого коммерческого оборота персональных данных на уровне штатов.



Тренд № 4. Защита интеллектуальных прав при обучении ИИ

В феврале 2025 г. Великобритания предложила разрешить «по умолчанию» использовать данные для обучения ИИ до тех пор, пока нет прямого запрета от правообладателя.

Тренд
Защита интеллектуальных прав при обучении ИИ



Тренд № 5. Антиконкурентные практики онлайн

В феврале 2025 г. продолжились расследования против Apple в Великобритании в связи со злоупотреблениями на рынке мобильных браузеров и облачного гейминга, а в Германии – в связи с манипулированием формами согласия на сбор данных в рекламных целях.

Тренд
Антиконкурентные практики онлайн

В феврале 2025 г. в России также произошло значимое событие в сфере регулирования цифровой экономики – предложены **новые правила аккредитации ИТ-компаний.**

Минцифры предложило изменить порядок аккредитации ИТ-компаний, необходимый для получения господдержки (например, сниженные налоговые ставки (5% вместо 25%) и страховые взносы (7,6% вместо 30%) и пр.):[1]

1. Аккредитацию запретят компаниям с 50% иностранного капитала и более. Такой запрет может снизить приток зарубежных инвестиций;

2. Компании с госучастием от 50% смогут получить аккредитацию, если 70% выручки компания получает от деятельности в сфере информационной безопасности. Операторы связи тоже смогут аккредитоваться, если доходы от ИТ превышают 50% общей выручки. Такая мера будет способствовать скорее не развитию ИТ-сектора, а дополнительной законной налоговой оптимизации отдельных крупных компаний, в том числе частных компаний с госучастием;

3. В список аккредитуемых организаций внесут компании в сфере квантовых коммуникаций и испытаний, аттестации и сертификации в сфере защиты информации. Включение квантовых технологий особенно актуально, так как в России активно ведутся разработки в этой сфере. Например, в сентябре 2024 г. в России создали 50-кубитный ионный квантовый компьютер[2]. На конец 2024 г. всего 6 стран мира, включая Россию, обладали такими квантовыми компьютерами;

4. Крупные ИТ-компании (выручка от 1 млрд руб., штат от 100 человек) для сохранения аккредитации обяжут сотрудничать с вузами в сфере ИТ-образования. Данная мера может способствовать повышению качества подготовки кадров, но увеличит административную нагрузку на ИТ-компании;

5. Малые ИТ-компании (до 1 млн руб. выручки, на рынке менее 3 лет) до конца 2025 г. освободят от проверок и подтверждения аккредитации. С 2026 г. такая льгота сохранится только для стартапов. Как следствие, после 2025 г. малые ИТ-компании без статуса стартапов могут столкнуться с трудностями при подтверждении аккредитации и потерять льготы.

Предлагаемые изменения корректируют действующие правила аккредитации ИТ-компаний, расширяя их охват и вводя дополнительные требования для вклада компаний в выполнение социальных функций бизнеса и власти.

[1] https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=154642#
[2] https://nauka.tass.ru/nauka/21937207

Ключевые аспекты

1. Ограничение работы DeepSeek

В феврале 2025 г. регуляторы стран Европы, США, Австралии[3] ввели ограничения на использование чат-бота DeepSeek, так как неясно, как компания хранит и обрабатывает данные пользователей. Также DeepSeek передает данные иностранных пользователей в Китай, что вызывает вопросы правомерности их передачи между юрисдикциями.

ОЭСР в Рекомендациях по ИИ 2019 г. указывает на необходимость обеспечения прозрачности сбора и обработки данных системами ИИ. Китай не присоединился к данным Рекомендациям. Ситуация с DeepSeek демонстрирует тренд на ужесточение контроля за иностранными цифровыми сервисами, которые работают с персональными данными иностранцев.

Опыт США

В январе-феврале 2025 г. ряд штатов США (Нью-Йорк[4], Техас[5], Вирджиния, Канзас и пр.) ввели запреты на использование DeepSeek на устройствах госслужащих, так как приложение может передавать данные пользователей правительству Китая. Интересно, что в 2022–2024 гг. в Техасе и Вирджинии уже вводились аналогичные запреты в отношении TikTok, WeChat, Rednote, Lemon8[6].

В Канзасе предложен специальный законопроект, запрещающий использование «опасных» платформ ИИ на государственных устройствах и сетях[7]. Госслужащие не смогут устанавливать или получать доступ к таким платформам на выданных им устройствах, а государственные сети должны блокировать их использование. Все госагентства обязаны удалять существующие аккаунты и прекратить работу с такими ИИ. Исключение делается только для правоохранительных органов и расследований в сфере кибербезопасности. Под «опасными» ИИ понимаются DeepSeek и любые модели, контролируемые Китаем, Россией, Ираном, КНДР, Кубой и Венесуэлой.

Опыт стран Европы

В январе-феврале 2025 г. ряд стран Европы запретили использование DeepSeek на государственных устройствах (Италия[8]) или выпустили рекомендации для граждан не использовать DeepSeek (Польша[9], Нидерланды[10], Лихтенштейн). В Германии началось расследование нарушения DeepSeek Общего регламента ЕС по защите данных (GDPR). Регуляторы предъявляют следующие претензии к DeepSeek:

1. отсутствие описания целей сбора данных пользователей, мер по обеспечению конфиденциальности и безопасности хранения данных (ст.12 GDPR и ст. 50 Закона ЕС об ИИ)

2. риск незаконной передачи данных пользователей из ЕС в Китай (нарушение ст.45 – 50 GDPR)[11]. DeepSeek собирает и хранит данные (IP-адреса, историю чатов, файлы, шаблоны нажатий клавиш) на серверах в Китае, который не имеет соглашения с ЕС о защите данных

3. отсутствие в ЕС официального представителя DeepSeek (ст. 27 GDPR). Данное требование касается всех компаний, собирающих персональные данные в ЕС и предоставляющих товары или услуги.

Опыт России

В России отсутствуют специальные требования к хранению данных, обрабатываемых системами ИИ. С одной стороны, Китай входит в список государств, обеспечивающих адекватную защиту прав субъектов персональных данных[12]. То есть в Китай можно передавать персональные

[3] https://www.protectivesecurity.gov.au/system/files/2025-02/PSPF-Direction-001-2025.pdf

[4] https://www.governor.ny.gov/news/governor-hochul-issues-statewide-ban-deepseek-artificial-intelligence-government-devices-and

[5] https://gov.texas.gov/news/post/governor-abbott-announces-ban-on-chinese-ai-social-media-apps

[6] Например, риск передачи указанными приложениями персональных данных по требованию китайского правительства представляет угрозу безопасности в соответствии со ст. 620.002(1) Государственного Кодекса Техаса https://www.governor.virginia.gov/media/governorvirginiagov/executive-actions/Governor-Glenn-Youngkin-Bans-DeepSeek-AI.pdf

[7] https://www.kslegislature.gov/li/b2025_26/measures/documents/hb2313_00_0000.pdf

[8] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10098477#english

[9] https://uodo.gov.pl/pl/138/3550

[10] https://www.autoriteitpersoonsgegevens.nl/actueel/ap-pas-op-met-gebruik-chatbot-deepseek

[11] Статьи 45–50 GDPR регулируют трансграничную передачу персональных данных за пределы ЕС. Передача возможна при наличии решения Европейской комиссии о достаточности мер защиты, использовании стандартных договорных положений, корпоративных правил или специальных разрешений.

[12] Приказ Роскомнадзора от 05.08.2022 № 128.

данные пользователей из России при уведомлении об этом Роскомнадзора.

С другой стороны, DeepSeek по-прежнему обязан соблюдать требования в части защиты данных, например, по локализации (хранению) данных российских пользователей на российских же серверах.

2. Обязанность платформ выплачивать чаевые

Опыт США

В феврале 2025 г. в США службы доставки Amazon[13] и DoorDash[14] должны оплатить штрафы в связи с невыплатой чаевых своим водителям доставки.

Еще в 2019 г. против Amazon началось расследование Федеральной торговой комиссией (FTC) по жалобе водителей на снижение оплаты труда. Сервис доставки Amazon Flex пообещал водителям заработок от 18 до 25 долл. в час, а также полную выплату чаевых. С 2016 г. Amazon решила сократить расходы на оплату труда водителей и снизила оплату ниже обещанной. Ставка формировалась алгоритмом с учетом размера чаевых таким образом, чтобы чаевыми покрывалась обещанная минимальная почасовая ставка. Amazon предоставляла общие сведения водителям о заработке – единую сумму без разделения на минимальную ставку оплаты труда и чаевые.

То есть Amazon обещала уплачивать 100% чаевых, которые оставляли клиенты водителям доставки, но на самом деле около трети чаевых направлялись на снижение расходов Amazon на рабочую силу – для субсидирования почасовых ставок зарплаты водителей. Иначе говоря, эти выплаты не были дополнительным заработком водителей. FTC вынесла решение о возврате водителям Amazon 61 млн долл.[15]. Теперь Amazon выплатит еще 3,95 млн долл. округу Колумбия за обман потребителей, которые думали, что их чаевые используются как дополнительный заработок для водителя.

Аналогичную схему использовала доставка DoorDash, которая внедрила схему «гарантированной оплаты». Перед тем как курьер принимал заказ на доставку, DoorDash указывала минимальную сумму заработка. Так, если стоимость доставки была 10 долл., а клиент оставлял 2 долл. чаевых, то водитель получал все равно 10 долл. (8 долл. – почасовая плата от DoorDash). И даже если клиент оставлял 9 долл., то тогда DoorDash уплачивала только 1 долл., доводя оплату до минимальной ставки в 10 долл. В результате в феврале DoorDash подписала соглашение с Нью-Йорком о возмещении 16,75 млн долл. чаевых 63 тыс. водителей за выполнение более 11 млн заказов.

Опыт России

В России отсутствует регулирование вопроса распределения чаевых, в том числе на платформах. Если найм осуществляется по трудовому договору, то в соответствии с Письмом Минфина[16] чаевые (официантов) считаются доходом в виде дарения и НДФЛ не облагаются, если переводятся физическим лицом непосредственно официанту.

А если чаевые переводятся сначала организации, то такой доход уже не считается дарением. При этом Минфин подчеркивает, что в этом случае работодатель может вычесть вознаграждение (комиссию) за прием чаевых по агентскому договору. Если применить указанный подход к платформам, то, например, таксопарки, работающие через платформы, вправе взимать комиссию за платеж с чаевых водителей.

Если лицо работает на платформе по гражданско-правовому договору, то платформы могут взимать комиссию с чаевых, выступая агентами или комиссионерами.

Между тем опыт зарубежных стран (ЕС, США, Франция) устанавливает специальные обязанности для платформ по выплате чаевых и информированию о их точном размере.

[13] https://oag.dc.gov/release/ag-schwalb-secures-395-million-amazon-resolve
[14] https://ag.ny.gov/press-release/2025/attorney-general-james-secures-1675-million-doordash-cheating-delivery-workers
[15] https://www.ftc.gov/system/files/documents/cases/1923123c4746amazonflexorder1.pdf

[16] Письмо Минфина России от 04.09.2019 № 03-04-05/67992 «Об НДФЛ и страховых взносах с сумм чаевых, перечисляемых (выплачиваемых) клиентами напрямую официантам или на расчетный счет организации (ресторана, кафе)».

3. Ограничение продажи персональных данных

Опыт США

В феврале 2025 г. в штате Вермонт рассматривался законопроект о защите конфиденциальности данных и наблюдении в Интернете[17]. Поскольку сегодня США – единственная юрисдикция, где на уровне штатов урегулирована продажа персональных данных, законопроект предусматривает для пользователей специальные права при продаже их данных компаниями, которые за предыдущий год обрабатывали данные не менее 25 тыс. человек, либо не менее 12,5 тыс. человек и 25% дохода компании приходилось на продажу персональных данных.

Компании обязаны предоставлять пользователю возможность отказаться от продажи его данных третьим лицам, а также их использование в таргетированной рекламе или цифровом профилировании. Компания должна предоставлять по запросу пользователя список третьих лиц, которым были переданы его данные. Практика продажи персональных данных признается высокорисковой для субъектов данных, поэтому компании обязаны проводить оценку защищенности обрабатываемых данных (data protection assessment) и раскрывать результаты такого внутреннего аудита по запросу генерального прокурора штата.

Законопроект продолжает тренд на ограничение продажи персональных данных, заданный в 2018 г. с принятием в Калифорнии требований к компаниям предоставлять пользователям право отказаться от продажи его данных третьим лицам. Сегодня во многих штатах принимаются законы о персональных данных, ужесточающие требования к условиям их продажи, например, в штате Вирджиния (Закон о защите данных потребителей 2021 г.), Юта (Закон о защите неприкосновенности частной жизни потребителя 2022 г.), Колорадо (Закон о неприкосновенности частной жизни 2023 г.). Требования фактически ограничивают крупные компании в продаже данных помимо воли пользователя, что предотвращает монополизацию рынка такими компаниями, накапливающими большие массивы данных.

Опыт России

В российской правовой практике не используется понятие «продажа персональных данных», но это не исключает проблемы серых схем торговли данными россиян. Например, в 2020 г. в банковском секторе на продажу было выставлено 9,2 млн записей о клиентах банков[18]. Основной источник данных на продажу – утечки в результате атак: в 2023 г. из банковского сектора утекло 170,3 млн записей[19]. Таким образом, в России существует теневой рынок торговли персональными данными, основными бенефициарами которого являются мошенники[20].

Однако данные пользователей представляют интерес и для законного бизнеса, например, для использования в маркетинговых целях. Поэтому в России актуален вопрос формирования списка законных оснований для передачи персональных данных между компаниями на коммерческой основе. Примечательно, что в национальных целях развития России до 2030 г. ставится задача формирования рынка данных, в который потенциально могут быть включены и персональные данные[21].

4. Защита интеллектуальных прав при обучении ИИ

В 2025 г. продолжается поиск оптимального регулирования прав интеллектуальной собственности (далее – ИС) при обучении ИИ, обеспечивая баланс между защитой правообладателей и потребностями разработчиков. В Мониторинге №5 2024 г. мы уже рассматривали подходы к решению этого вопроса в Китае, ЕС, Франции, Италии, США.

Опыт США

В феврале 2025 г. принято судебное решение по делу Thomson Reuters и West Publishing против Ross Intelligence о нарушении авторских прав на юридические

[17] https://legiscan.com/VT/text/H0208/id/3116104

[18] https://garda.ai/blog/news/analiz-tenevogo-rynka-baz-dannykh-bankov-za-2020-god

[19] https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D0%B8%D0%B7_%D0%B1%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8

[20] https://garda.ai/blog/news/analiz-tenevogo-rynka-baz-dannykh-bankov-za-2020-god

[21] http://www.kremlin.ru/acts/news/73986

аннотации и систему классификации правоприменительных решений (судебных, административных и др.) платформы Westlaw[22]. Ross создала инструмент для юридических исследований на основе ИИ, незаконно используя материалы истцов для обучения своей системы.

Суд признал факт прямого копирования Ross данных с Westlaw в нарушение Закона об авторском праве[23], установив, что Thomson Reuters владеет авторскими правами не только на тексты, но и на их отбор и организацию. Суд отклонил доводы Ross о добросовестном использовании контента[24] (fair use), поскольку ИИ использовался в коммерческих целях и перерабатывал данные полностью, а не частично[25]. Ross создала конкурентный продукт на основе незаконно полученного контента, принадлежащего Thomson Reuters, и генерировала на его основе собственные данные на том же рынке.

Суд также подтвердил, что аннотации Westlaw, сгенерированные ИИ, обладают достаточной оригинальностью для защиты авторским правом. То есть владелец системы ИИ (Thomson Reuters) признается правообладателем сгенерированного контента. Таким образом, использование в ИИ данных без разрешения правообладателей нарушает закон даже при ссылке на fair use.

Также в феврале 2025 г. в Калифорнии опубликован законопроект о повышении прозрачности использования данных для обучения ИИ. Предлагается требовать от разработчиков генеративного ИИ документировать использование защищенных авторским правом материалов при обучении ИИ, указывать владельцев авторских прав и хранить данные о фактах использования таких данных и их владельцах в течение коммерческого использования модели ИИ и еще 10 лет после. Разработчики по требованию правообладателя должны предоставлять список использованных материалов в течение 7 дней[26].

Опыт Великобритании

В феврале 2025 г. проведены публичные обсуждения планов по защите прав ИС при использовании ИИ[27]. Великобритания рассматривает 4 подхода к регулированию ИС в контексте обучения ИИ: (1) отсутствие специального регулирования; (2) обязательное лицензирование; (3) право кому угодно использовать данные для обучения ИИ; или (4) такое же право, но с возможностью правообладателя запрещать использование, и с обязанностью разработчика обеспечивать прозрачность использования данных и отчитываться об их использовании.

Великобритания выбрала 4-й подход – соответственно, планируется внедрение модели, при которой авторы смогут заранее запрещать использование своих работ, а при отсутствии такого запрета их контент можно будет свободно применять. Это позволит правообладателям зарабатывать на лицензировании, а разработчикам — работать с большими объемами данных. Разработчики ИИ должны раскрывать, на каких данных обучаются их модели (аналогично нормам Закона ЕС об ИИ).

Существующие средства защиты авторских прав, как запреты для роботов[28], недостаточны. Они позволяют блокировать доступ к общедоступным сайтам в сети интернет, но не защищают отдельные произведения. Поэтому Великобритания изучает способы усиления контроля над данными через метаданные с запретом на сбор контента[29], разработка стандартов учета прав доступа, копирования и т.д., а также централизованные реестры ограничений. Предлагается передавать права организациям коллективного управления для лицензирования и распределения платежей.

Опыт России

В России отсутствует правовое регулирование защиты прав ИС при

[22] https://www.lawnext.com/wp-content/uploads/2025/02/2025-02-11-Memorandum-dckt-770_0.pdf
[23] Ст. 410(c) раздела 17 Свода законов США.
[24] Допустимость использования объектов интеллектуальной собственности иных лиц без прямого согласия для научных, учебных, культурных и иных аналогичных некоммерческих целей.
[25] Ст. 107 раздела 17 Свода законов США.
[26] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB412
[27] https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence
[28] Например, фильтры, выявляющие программы – роботов по сбору данных и не позволяющие им получить доступ к сайту.
[29] То есть проставление в метаданных пометок («флагов») для систем ИИ или их разработчиков, которые показывают разрешен ли данный набор метаданных к использованию для обучения ИИ.

обучении ИИ. В феврале 2025 г. планировалось утвердить обновленную Концепцию регулирования ИИ, однако сведения о таком утверждении отсутствуют. Проект Концепции ставит задачу проработки вопросов охраны прав ИИ на произведения, созданные с использованием ИИ, маркировки таких произведений для прозрачности их происхождения. Предлагается, чтобы ответственность за результаты работы ИИ нес человек или организация, контролирующие систему и принимающие решения об её использовании[30]. То есть сейчас в России отсутствует специальное регулирование, но если будут реализованы описанные выше планы из проекта Концепции, то российский подход будет включать предоставление разрешений «по умолчанию» и с требованиями к раскрытию информации, как это принято в ЕС и планируется в Великобритании.

5. Антиконкурентные практики онлайн

В феврале 2025 г. продолжилось расследование злоупотреблений Google и Apple на рынке мобильных браузеров и облачных игр[31]. Управление по конкуренции и рынкам (CMA) выявило злоупотребления:

1. Apple требует, чтобы мобильные браузеры на устройствах iOS использовали браузерный движок от Apple – WebKit. При этом WebKit не предоставляет те же функции для конкурирующих браузеров, которые предоставляет браузеру Apple Safari. Так, ограничена возможность браузеров Mozilla и Vivaldi предлагать пользователям дополнительные функции безопасности, как «режим безопасного просмотра» (направляются предупреждающие сообщения о потенциально опасных сайтах или загрузках), функции полноэкранного воспроизведения видео и пр.;

2. Apple ограничивает функционал и снижает трафик «прогрессивных приложений»[32] – версия веб-сайта, сохраняемая на главном экране устройства как приложение. Это ограничивает запуск приложений разработчиками, при этом такие приложения могут работать в любой операционной системе, а их разработка дешевле и проще для компаний[33];

3. Apple ограничивает функцию просмотра веб-страниц в приложениях, работающих на WebKit, снизив трафик;

4. Apple заключила соглашение с Google о распределении доходов, по которому Google выплачивает Apple долю доходов, получаемых от трафика в Safari и Chrome на iOS от поисковой рекламы.

Также CMA планирует оценить влияние действий Apple на конкуренцию на рынке облачного гейминга[34]. Например, Apple требует:

– чтобы каждая игра отправлялась в App Store как отдельное приложение – ограничивается создание на iOS приложений-агрегаторов с доступом к множеству потоковых игр;

– использовать платежные системы Apple для совершения транзакций внутри игр, взимая комиссию 30%.

Опыт Германии

В феврале 2025 г. Федеральное управление по борьбе с картелями оценило Фреймворк Apple по прозрачности при отслеживании в приложениях (App Tracking Transparency)[35]. Фреймворк – это требования к разработчикам о правилах информирования пользователей об использовании их персональных данных, в частности, в рекламных целях. Перед использованием данных для рекламных целей разработчики должны получить согласие пользователя на это, особенно если создают бесплатные приложения, финансирующиеся за счет рекламы.

Было выявлено, что формулировки и дизайн таких согласий различались для приложений Apple и для приложений сторонних разработчиков так, чтобы поощрять пользователей разрешать сбор данных собственными приложениями Apple и

[30] https://www.pnp.ru/social/koncepciyu-regulirovaniya-iskusstvennogo-intellekta-obnovili.html

[31] https://digitalpolicyalert.org/event/27509-cma-issued-a-summary-of-the-provisional-decision-report-pdr-response-hearing-with-google

[32] Progressive web apps

[33] Такие приложения не обязательно скачивать из App Store – можно сайт сохранить на экране телефона как обычное приложение (в основном бесплатно).

[34] https://assets.publishing.service.gov.uk/media/6687b9fd899a6f92e5d9cd46/WP6_-_Cloud_gaming_services__nature_of_competition_and_requirements_for_native_apps_on_mobile_devices.pdf

[35] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2025/02_13_2025_ATTF.html?nn=52004

отказывать в разрешении сторонним приложениям. Например, для сторонних приложений требовалось получить отдельное согласие пользователей на использование и объединение их данных разными сервисами внутри компании-разработчика в рекламных целях, которое запрашивалось во всплывающем окне при первом запуске приложения. Однако ограничения на объединение пользовательских данных из разных сервисов в экосистеме Apple (App Store, Apple ID, с устройств) в рекламных целях отсутствовали, запросы Apple на согласие вообще не раскрывали методы обработки данных между сервисами Apple. В итоге разработчики сторонних приложений вынуждены предлагать пользователям до 4 всплывающих окон, чтобы получить все согласия, тогда как для приложений Apple – только 2. Расследование еще продолжается.

Опыт России

В России Принципы взаимодействия участников цифровых рынков ФАС не охватывают практики, связанные со злоупотреблением доминирующим положением за счет различных технологий, как замедление трафика браузеров, ограничения работы прогрессивных приложений, манипулирования формами согласия на сбор данных.