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

- **НДС на цифровые услуги в ЕС**
- **ИИ в сфере жилья**
- **Безопасность детей в интернете и бизнес**
- **Новые требования кибербезопасности в ЕС**
- **Госзакупки высокорискового ИИ**

Мониторинг №3 (15) (Март 2025)

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

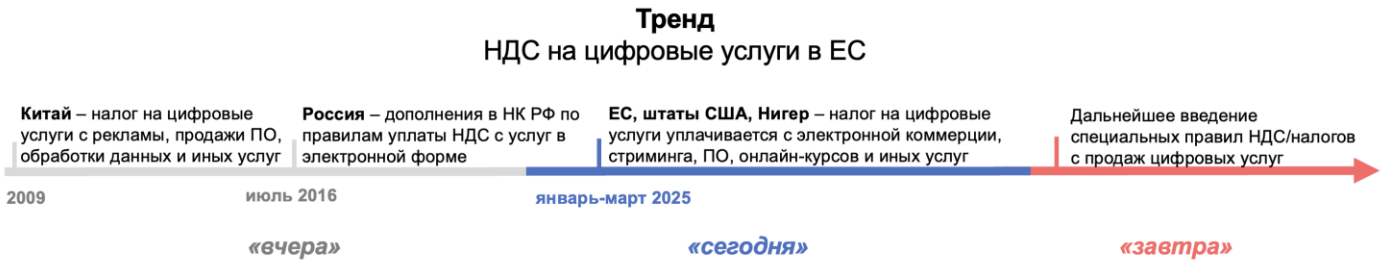
Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Магомедова О.С., науч. сотр. Черновол К.А.

«Дух пряный марта был в лунном круге,
Под талым снегом хрустел песок.
Мой город истаял в мокрой вьюге,
Рыдал, влюбленный, у чьих-то ног.»
А. Блок

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

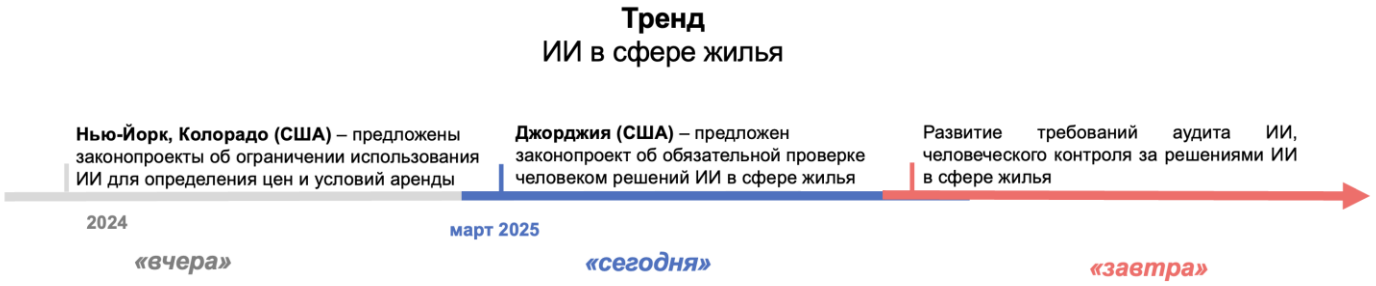
Тренд № 1. НДС на цифровые услуги в ЕС

В марте 2025 г. в ЕС приняты поправки в Регламент о единой системе НДС, устанавливающие требования к хранению платформами краткосрочной аренды жилья и пассажирских перевозок информации о своих бизнес-пользователях. Это необходимо, чтобы платформы (как Airbnb или Uber) сами платили НДС за тех, кто предоставляет услуги через них.



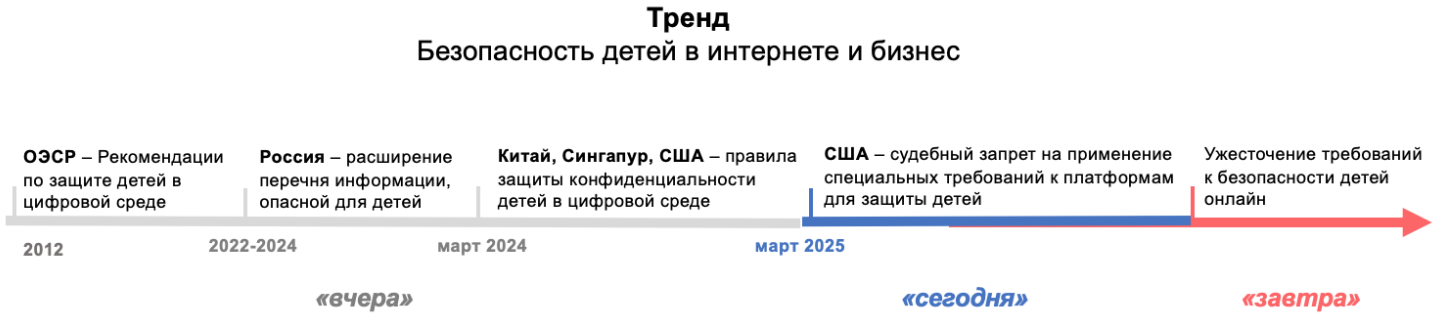
Тренд № 2. ИИ в сфере жилья

В марте 2025 г. в штате Джорджия (США) было предложено ограничить использование ИИ для определения цен на аренду жилья.



Тренд № 3. Безопасность детей в интернете и бизнес

Усиление требований безопасности детей в интернете (рассматривался в Мониторинге №4 за 2024 г.) может столкнуться с сопротивлением бизнеса. В марте 2025 г. в штате Калифорния (США) суд вынес судебный запрет на применение норм Кодекса «О дизайне, который соответствует возрасту пользователей» (для несовершеннолетних), признав его противоречащим Конституции США.



Тренд № 4. Новые требования кибербезопасности в ЕС

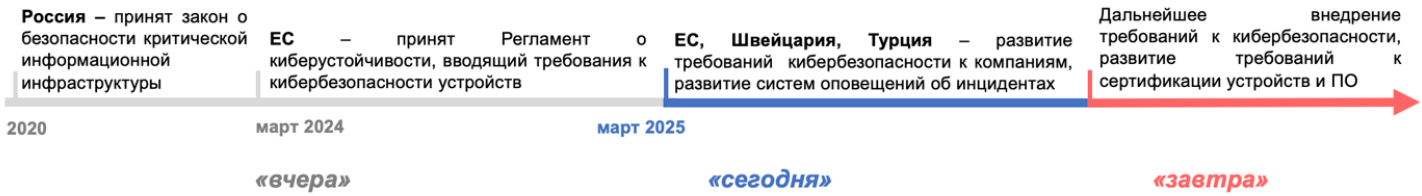
В марте 2025 г. в ЕС было опубликовано описание товаров и ПО, которые подпадут под требования кибербезопасности. Без соблюдения таких требований товары не смогут продаваться

на европейском рынке. Предъявление требований кибербезопасности непосредственно к производимым товарам, а не в целом к компании-производителю – подход, неимеющий в настоящее время аналогов в других юрисдикциях.

Другие же юрисдикции в марте 2025 г сосредоточились на развитии уже традиционных для стран инструментов кибербезопасности: так в Швейцарии и Турции введены требования к оповещению госорганов об инцидентах.

Тренд

Требования кибербезопасности устройств



Тренд № 5. Госзакупки высокорискового ИИ

В марте 2025 г. ЕС предложил модельные контрактные положения для договоров госзакупок высокорисковых систем ИИ.

Тренд

Госзакупки высокорискового ИИ

В марте 2025 г. в России введен **запрет на распространение рекламы на платформах нежелательных и запрещенных организаций**[1], в частности тех, чья деятельность признана экстремистской и террористической. Фактически это означает запрет рекламы через ресурсы Meta[2] (Instagram и Facebook), кроме WhatsApp.

[1] Федеральный закон от 07.04.2025 № 72-ФЗ "О внесении изменений в статью 12 Федерального закона "О противодействии экстремистской деятельности" и Федеральный закон "О рекламе"

[2] Деятельность компании Meta признана экстремистской и запрещена на территории Российской Федерации.

Ключевые аспекты

1. НДС на цифровые услуги в ЕС

Опыт ЕС

В марте 2025 г. приняты поправки в Регламент ЕС № 282/2011[3]. Инициатива ЕС «НДС в цифровую эпоху»[4] (ViDA) расширяет введенную в 2021 г. концепцию «признанного поставщика» (deemed supplier). Концепция означает, что в определенных случаях платформы считаются ответственными за уплату НДС за своих бизнес-клиентов, как если бы эти платформы сами продавали товары или услуги. Раньше эта концепция применялась к платформам для продажи товаров, в первую очередь импортных. С июля 2028 г. эти же правила распространят на платформы, через которые предоставляются услуги краткосрочной аренды жилья (до 30 дней), пассажирских перевозок. Такие платформы будут начислять и уплачивать НДС за арендодателей и таксистов. Однако, если платформа предоставляет только услуги по размещению рекламы, перенаправлению пользователей на ресурсы третьих лиц или обработке платежей, она не будет считаться «deemed supplier»[5].

Также платформы освобождаются от ответственности за неправильный расчет НДС, если они действовали на основании недостоверной информации от поставщика и не могли знать о её недостоверности. Платформы обязаны собирать и хранить дополнительную информацию о поставщиках и транзакциях, даже если режим deemed supplier не применяется, — это необходимо для сопоставления с данными о платежах, собираемых в рамках новой системы налогового контроля в отношении лиц, предоставляющих услуги через платформы.

Платформа выполняет требования признанного поставщика при наличии у бизнес-пользователя VAT-номера,[6] а если VAT-номера нет, то обязанность по уплате НДС несет сам бизнес-пользователь.

Опыт США (уровень штатов)

В Мэриленде в марте 2025 г. опубликован законопроект, предполагающий введение налога с продаж в размере 3% на информационные услуги, включая разработку веб-сайтов и решений для облачного хранения данных, обработку данных, услуги проектирования компьютерных систем интернет-публикаций, онлайн-вещания, поисковиков и сопутствующие услуги[7].

При этом в Нью-Йорке еще в январе 2025 г. предложены специальные косвенные налоги на услуги:

1) цифровой рекламы. Ставки от 2,5% до 10% в зависимости от объема валового дохода компании от всех источников за год[8].

2) акцизный налог на деятельность по сбору данных[9] для коммерческих сборщиков данных, обрабатывающих информацию от более чем 1 млн потребителей в месяц[10].

Опыт Нигера

С 2025 г. в Нигере ввели НДС в размере 19% на продажи товаров и услуг, осуществляемые как через иностранные, так и через местные платформы электронной коммерции, а также на комиссии, получаемые операторами этих платформ. Для выполнения своих налоговых обязательств платформы-нерезиденты обязаны назначить представителя, проживающего в Нигере[11].

Опыт России

В России с 2017 г. действует ст. 174.2 НК РФ, которая регулирует порядок налогообложения услуг, оказываемых в

[3] Регламент, устанавливающий меры по реализации Директивы 2006/112/ЕС об общей системе налога на добавленную стоимость.
[4] EU VAT in the Digital Age, НДС в ЕС в цифровую эпоху.
[5] https://data.consilium.europa.eu/doc/document/ST-14963-2024-INIT/en/pdf
[6] Индивидуальный идентификационный номер налогоплательщика, зарегистрированного для целей начисления и уплаты НДС..
[7] https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/hb1554
[8] https://www.nysenate.gov/legislation/bills/2025/S173
[9] Сбор, использование, обработка, продажа или иная передача данных, которые идентифицируют, относятся, описывают или могут быть обоснованно связаны с пользователями.
[10] https://www.nysenate.gov/legislation/bills/2025/A1434
[11] https://www.impots.gouv.ne/media/loi/ORDONNANCE%20N%202024-59%20LOI%20DE%20FINANCES%202025..pdf

электронной форме, например, предоставления прав на использование программ для ЭВМ и баз данных через интернет, включая обновления и дополнительные функции, а также оказания рекламных услуг в сети. Данная норма введена для создания единых правил налогообложения цифровых услуг в ЕАЭС.

Иностранные организации, предоставляющие электронные услуги физическим лицам в России, по общему правилу обязаны самостоятельно исчислять и уплачивать НДС. При оказании таких услуг российским организациям или индивидуальным предпринимателям обязанность по уплате НДС возлагается на российских покупателей в качестве налоговых агентов.

2. ИИ в сфере жилья

Опыт США

В марте 2025 г. в штате Джорджия (США) был предложен законопроект[12], запрещающий использование ИИ в жилищной сфере, если (1) генерирование решений о продаже, аренде, финансировании жилья (например, ипотека), а также (2) оказание посреднических услуг (например, платформенных) или связанных услуг (например, поставки приложений с ИИ для продажи или аренды жилья) происходит без человеческого участия – без проверки решений ИИ ответственным лицом. Предложено введение ответственности за случаи, если пользователь не предупрежден, что при генерировании решений использовался ИИ или иной автоматизированный инструмент.

Аналогичные законопроекты предлагаются и в других штатах. Например, еще в 2024 г. в Колорадо было предложено признать недобросовестной или обманной торговой практикой использование алгоритмов при установлении размера арендной платы (законопроект отклонен)[13].

В Нью-Йорке[14] предлагалось (законопроект отклонен) запретить арендодателю использовать автоматизированные инструменты принятия решений, в том числе ИИ, если для такого инструмента минимум раз в год не проводится разработчиком анализ оценки фактического воздействия инструмента. Результаты оценки воздействия должны быть опубликованы на сайте арендодателя до начала использования такого инструмента.

Оценка воздействия включает проверку степени, когда использование автоматизированного инструмента может привести к неблагоприятному воздействию для группы лиц по признаку пола, расы, этнической принадлежности и пр. Арендодатель должен уведомлять арендатора об использовании ИИ, о характеристиках арендатора, которые будет учитывать инструмент при принятии решений об аренде, предоставлять информацию о типе, источнике используемых данных и политике хранения данных арендодателем. Если арендодателю отказано в аренде жилья – объяснить причину отказа.

В настоящее время в Нью-Йорке рассматривается законопроект A 10020[15] в отношении алгоритмов ценообразования – любых вычислительных процессов, включая ИИ, обрабатывающих данные для рекомендации цен или условий в сфере жилья. Предлагается запретить при установлении размера арендной платы применять инструменты алгоритмического ценообразования, которые используют или обучались на закрытых данных конкурентов. К таким данным относятся непубличные данные, которыми могут обмениваться арендодатели, например, если используют одно и то же приложение для установления цен на жилье, предоставляя информацию о стоимости жилья, о его качестве (количество комнат, состояние), предыдущих контрактах аренды жилья.

Во многом такое регулирование и попытка ограничить использование ИИ связаны с рисками антиконкурентного поведения и ценового сговора, которые приводят к росту цен на жилье. Например, из-

[12] https://www.legis.ga.gov/legislation/71101

[13] https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:CO2024000H1057&verid=CO2024000H1057_20240110_0_I&

[14] https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:NY2023000A7906&verid=NY2023000A7906_20230719_0_I&

[15] https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:NY2023000A10020&verid=NY2023000A10020_20240501_0_I&

за использования приложении с ИИ, которые помогают арендодателям устанавливать цены на жилье, цены на рынке аренды недвижимости США выросли на 20% с 2020 по 2024 гг.

Опыт России

В России ИИ используется платформами поиска жилья (например, на Циан), но специальное регулирование отсутствует.

3. Безопасность детей в интернете и бизнес

Опыт США

В марте 2025 г. суд штата Калифорния вынес временный судебный запрет на применение Кодекса Калифорнии о дизайне, соответствующем возрасту пользователя (вступил в силу с января 2025 г.),[16] признав Кодекс неконституционным. Кодекс устанавливает требования по защите несовершеннолетних пользователей[17]. Субъекты – крупные цифровые платформы с доходом свыше 25 млн. долл. или компании, продающие данные более 100 тыс. пользователей.

Ассоциация Netchoice (входят Google, Meta[18], Amazon, Netflix) обратилась в суд Калифорнии с иском о нарушении Кодексом поправок к Конституции США и других законов, так как Кодекс:

1) нарушает 1-ю поправку к Конституции США о свободе слова, поскольку ограничивает оборот информации. Свобода слова в конституционном праве США трактуется широко, включая право выражать мнение через информационные ресурсы – любые требования, связанные с обязательной модерацией контента, могут ограничивать свободу слова.

Кодекс возлагает на платформы функции цензоров – обязывает оценивать, какой контент является «вредным» или может причинить «материальный ущерб здоровью ребенка». Платформы, ограничивая доступ к информации «вредной для ребенка», часто на свое усмотрение принимают решение о том, какую информацию ограничить, так как отсутствуют четкие критерии «вредной информации»;

2) нарушает 4-ю поправку к Конституции США – право на неприкосновенность частной жизни за счет требования о верификации возраста пользователя. Такое требование влечет необходимость сбора как можно большего количества персональных данных, что противоречит принципу «минимизации сбора данных»;

3) нарушает 14-ю поправку к Конституции США о надлежащей правовой процедуре, поскольку содержит множество неясных понятий: что такое «материальный ущерб здоровью ребенка», «вредный контент»? Кодекс содержит требование обработки данных строго для одной цели, однако при этом допускает использовать данные для новой цели, но только при наличии «весомого доказательства», если такое новое использование данных происходит в «лучших интересах ребенка». При этом не раскрываются критерии «лучших интересов» и «весомости доказательства»;

4) вступает в противоречие с другими законами. Например, ребенком считается лицо до 18 лет, что противоречит Закону1998 г. о неприкосновенности частной жизни детей в интернете, включающему в категорию «детей» пользователей в возрасте до 13 лет.

Суд Калифорнии счел доводы NetChoice обоснованными для того, что выпустить временный запрет на применение спорных норм, который будет действовать до принятия судом окончательного решения по существу дела.

Опыт России

В России безопасность детей в интернете регулируется положениями ФЗ №436 «О защите детей от информации» 2010 г. Закон регулирует только вопросы демонстрации детям опасной информации, такой как пропаганда педофилии или информация, мотивирующая к смене пола и пр. Закон не предусматривает требований об обеспечении инструментов родительского контроля за информационной безопасностью

[16] https://netchoice.org/wp-content/uploads/2024/11/2024-11-12-NetChoice-v-Bonta-2024-Complaint-FILED.pdf

[17] Например, проверка возраста пользователя (Age estimation requirement), настройки защиты данных по умолчанию (Default privacy settings), информирование о контроле и мониторинге (Monitoring signal)

[18] Признана экстремистской организацией и запрещена на территории России

ребенка. Закон об информации возлагает на социальные сети обязательство по мониторингу контента на платформе для предупреждения распространения запрещенной в России информации, включая информацию опасную для детей (п. 5 ст. 10.6 ФЗ №149). Соцсети обязаны формировать публичные отчеты по результатам мониторинга.

4. Новые требования кибербезопасности в ЕС

Опыт ЕС

В марте 2025 г. Европейская комиссия опубликовала проект исполнительного регламента, который сформулировал технические описания категорий продукции, которая относится к «важной» и «критической»,[19] и к которой будут предъявляться требования Союза о кибербезопасности. Ожидается, что принятие проекта повысит требования и стоимость для входа компаний на европейский рынок.

Формирование требований к кибербезопасности в ЕС началось еще с принятия в 2020 г. Стратегии кибербезопасности. Было предложено развивать требования к управлению кибер-рисками в компаниях и на отдельных объектах инфраструктуры, а также требования к кибербезопасности конечной продукции (товары и ПО), которую используют компании и потребители. Повышенное внимание к конечной продукции объясняется изменением парадигмы хранения, обработки и передачи данных: от хранения и обработки в централизованных хранилищах данных к развитию периферийных вычислений, т.е. когда данные обрабатываются непосредственно на устройстве.

В октябре 2024 г. в ЕС был принят Регламент о киберустойчивости[20], предусматривающий требования ко всем производителям и импортерам товаров с «цифровыми элементами» о внедрении стандартов кибербезопасности продукции[21]. К таким товарам отнесены программные или аппаратные продукты, имеющие функционал удаленной обработки данных. Иными словами, любой товар, предполагающий подключение к Интернету (или к иной сети) для обработки данных, подпадает под регулирование. Регламент распространяется как на потребительские товары (например, умные товары для дома), так и на промышленные.

В регламенте выделены 3 категории товаров, к которым предъявляются повышенные требования кибербезопасности:

1) важная продукция (класс 1) – роутеры, программы – менеджеры паролей, ВПН и др. К такой продукции предъявляются требования соответствия европейскому стандарту кибербезопасности, но без сертификации такого соответствия, или, если такого стандарта не существует, – то общим требованиям, которые будут установлены ЕК;

2) важная продукция (класс 2) – брандмауэры[22]; гипервизоры[23] и др. К такой продукции также предъявляются требования о соответствии стандартам, однако соответствие должно быть сертифицировано сторонней организацией (например, бизнес-ассоциацией);

3) критическая продукция – смарт-карты (банковские карточки; удостоверение личности; карточки, которые используются как электронные кошельки или устройства хранения ключей), шлюзы интеллектуальных счетчиков, используемые для измерения электроэнергии[24] и др. К такой продукции уже предъявляются требования по сертификации по схеме European Common Criteria (EUCC), предполагающей сертификацию только у организаций, получивших специальную аккредитацию у государственных органов.

В отношении остальных категорий товаров производитель самостоятельно оценивает риски кибербезопасности. По оценкам ЕК, к этой категории будет

[19] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_en

[20] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

[22] ПО, которое фильтрует входящую информацию и не пропускает вредоносный контент и вирус.

[23] ПО, которое используется для запуска нескольких операционных систем на одном устройстве и отвечает за предоставление вычислительных ресурсов каждой из операционных систем в процессе использования.

[24] Устройство связи, способное передавать и получать данные для целей информации, мониторинга и контроля.

относиться до 90% всей продукции. Требования регламента начнут действовать с декабря 2027 г.

В рамках проекта исполнительного регламента, опубликованного в марте 2025 г., уточняется, что относится к той или иной продукции. Это позволяет компаниям лучше понимать вводимые требования. Например, к менеджерам паролей относятся как ПО, так и аппаратные устройства, предназначенные для хранения паролей.

Опыт Швейцарии

В марте 2025 г. в Швейцарии было принято положение, которое обязует операторов критически важной инфраструктуры (поставщики энергии и питьевой воды, транспортные компании, кантональные и коммунальные администрации) сообщать о кибератаках в Национальный центр кибербезопасности (NCSC) в течение 24 часов с момента обнаружения происшествия[25].

Обязательному сообщению подлежат кибератаки, которые угрожают функционированию критически важной инфраструктуры, привели к утечке или изменению информации, либо сопровождаются вымогательством, угрозами или принуждением. Операторы, не выполнившие требование, могут быть оштрафованы.

После первоначального уведомления в течение 24 часов у организаций будет 14 дней для предоставления полной информации о происшествии.

Примечательно, что аналогичная система уже создана в ЕС, об этом мы упоминали в Мониторинге №3 за 2024 г. Кроме того, описанное выше регулирование ЕС о цифровых элементах, также предполагает введение системы оповещения производителями такой продукции о выявленных уязвимостях – требование будет применяться с сентября 2026 г.

Опыт Турции и Вьетнама

В марте 2025 г. в Турции вступил в силу закон о кибербезопасности, предусматривающий обязанности и меры для отдельных компаний и государственных органов по внедрению мер кибербезопасности, включая сообщение о случившихся инцидентах, возможности приобретения сертифицированных продуктов кибербезопасности и пр.[26]

Правительство Вьетнама завершило публичные консультации в части введения для отдельных компаний обязанности по внедрению системы управления рисками киберопасности, проведения регулярных аудитов безопасности и разработки планов реагирования на инциденты для смягчения киберугроз[27].

Опыт России

В России с 2017 г. действует Закон «О безопасности критической информационной инфраструктуры», который также, как и принятые аналогичные нормы в ЕС, Швейцарии и других странах, предполагает механизм информирования о компьютерных инцидентах, а также требует обеспечивать безопасность значимых объектов критической информационной инфраструктуры.

5. Госзакупки высокорискового ИИ

Опыт ЕС

В марте 2025 г. ЕС опубликовал модельные контрактные положения для госзакупок высокорисковых систем ИИ (MCC-AI-High-Risk)[28], которые госзаказчики могут включать в договоры с поставщиками ИИ-систем. Регламент ЕС об ИИ (AI Act)[29] к высокорисковым ИИ относит системы, связанные с критической инфраструктурой, биометрией, правами человека, образованием, трудоустройством и правосудием.

MCC-AI-High-Risk устанавливают типовые контрактные обязательства поставщиков, включая создание системы управления рисками, обеспечение качества

[25] https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-104400.html
[26] https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm
[27] https://xaydungchinhsach.chinhphu.vn/toan-van-du-thao-nghi-dinh-quy-dinh-chi-tiet-mot-so-dieu-va-bien-phap-thi-hanh-luat-du-lieu-du-thao-2-119250123120619898.htm
[28] https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

данных, прозрачность работы ИИ-системы, человеческий контроль за генерируемыми ИИ решениями и пр. в соответствии с требованиями AI Act, (рассматривались в Мониторинге №3 за 2024 г.).

С точки зрения закупок внимание уделяется правам на используемые данные. MCC-AI-High-Risk разграничивают данные заказчика и поставщика. Данные заказчика (переданные госорганом или специально для него собранные) остаются в его собственности, а поставщик не вправе использовать их вне рамок договора и обязан по требованию вернуть или уничтожить их. Данные поставщика (например, модели и датасеты для обучения) остаются под контролем поставщика, однако заказчику предоставляется неисключительная лицензия[30] на их использование в рамках эксплуатации системы.

Для обеспечения соблюдения всех требований контракта заказчик вправе на всех этапах (разработка, внедрение и эксплуатация) запрашивать у поставщика подтверждающую документацию и проводить аудит.

MCC-AI-High-Risk обязывают включать в исходную цену контракта все затраты, связанные с выполнением требований AI Act, включая расходы на аудит, подготовку сопроводительной документации, внедрение механизмов прозрачности и пр.

Опыт США

В США в сентябре 2024 г. Административно-бюджетное управление Администрации Президента (OMB) выпустило Меморандум M–24–18[31] по стандартизации закупок систем ИИ федеральными агентствами. Документ выделяет закупки особенног рискованного ИИ:

- правозатрагивающих систем, влияющих на права человека (например, автоматический отбор при трудоустройстве). Контрактные условия должны предусматривать обязательные меры прозрачности, механизмы исправления и непременный человеческий пересмотр спорных решений;
- систем, затрагивающих безопасность – влияющих на здоровье и жизнь граждан, инфраструктуру и др. (например, системы управления транспортом, энергетикой). Закупка должна сопровождаться полным доступом к информации о разработке системы, позволяющей оценивать её надежность и предотвращать негативные последствия.

В контрактах рекомендовано фиксировать следующие условия для контроля ИИ:

- использование тестовых наборов данных, сформированных госзаказчиком, для независимой проверки поставляемого ИИ. Такие наборы должны быть недоступны для подрядчика заранее и максимально близко имитировать реальные данные, с которыми система ИИ будет работать;
- обязанность подрядчика предоставлять доступ для проведения госзаказчиком испытаний в условиях, приближенных к реальным условиям использования системы (аналогичное требование в ЕС);
- право госзаказчика публиковать методы и результаты тестирования системы (не нарушая прав интеллектуальной собственности поставщика).

Меморандумом установлены требования для:

- генеративного ИИ – по обязательной маркировке контента (например водяными знаками), предоставлению подробной документации о методах обучения и тестирования и пр.;
- биометрического ИИ, осуществляющего идентификацию личности – требуется проведение независимых испытаний на точность распознавания, соблюдение стандартов качества входных данных, установление порогов точности поиска и обязательное ведение защищённых журналов запросов и идентификаций.

Меморандум закрепляет обязанность подрядчиков уведомлять агентства о серьёзных инцидентах, связанных с работой ИИ, для оперативного реагирования и предотвращения негативных последствий.

[30] По неисключительной лицензии поставщик сохраняет право предоставлять аналогичные права на использование моделей и датасетов другим заказчикам.

[31] https://www.whitehouse.gov/wp-content/uploads/2024/10/M-24-18-AI-Acquisition-Memorandum.pdf

Опыт России

В России на данный момент отсутствует специализированное регулирование для госзакупок ИИ-систем. Однако утверждён ГОСТ Р 71752—2024 «Искусственный интеллект. Техническое задание»[32], устанавливающий требования к техническим заданиям на закупку и внедрение систем ИИ, включая государственные и коммерческие закупки. Минцифры РФ разработало Методические рекомендации по цифровой трансформации[33], рекомендующие интегрировать ИИ в бизнес-процессы государственных организаций, формировать стратегии по применению ИИ и оценке эффективности внедряемых решений.

[32] https://docs.cntd.ru/document/1310068312

[33]https://digital.gov.ru/uploaded/files/140020231228obnovlennyiemetodicheskierekomendatsiiv12sokraschennyie-1.pdf