ИНСТИТУТ ЭКОНОМИЧЕСКОЙ ПОЛИТИКИ имени Е.Т. ГАЙДАРА

Лаборатория анализа лучших международных практик

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

Борьба с антиконкурентными практиками, кибербезопасность, новые законы для искусственного интеллекта

Мониторинг №3 (Март 2024)

Мониторинг подготовлен коллективом экспертов Института экономической политики имени Е. Т. Гайдара (Института Гайдара):
Левашенко А.Д., с.н.с. лаборатории анализа лучших международных практик Института Гайдара;
Гирич М.Г., н.с. лаборатории анализа лучших международных практик Института Гайдара;
Ермохин И.С., н.с. лаборатории анализа лучших международных практик Института Гайдара;
Магомедова О.С., н.с. лаборатории анализа лучших международных практик Института Гайдара;
Малинина Т.А., с.н.с лаборатории анализа лучших международных практик Института Гайдара

APRIL 10, 2024

«А вот теперь весна, так и мысли все такие приятные, острые, затейливые, и мечтания приходят нежные; все в розовом цвете»

Ф.М. Достоевский

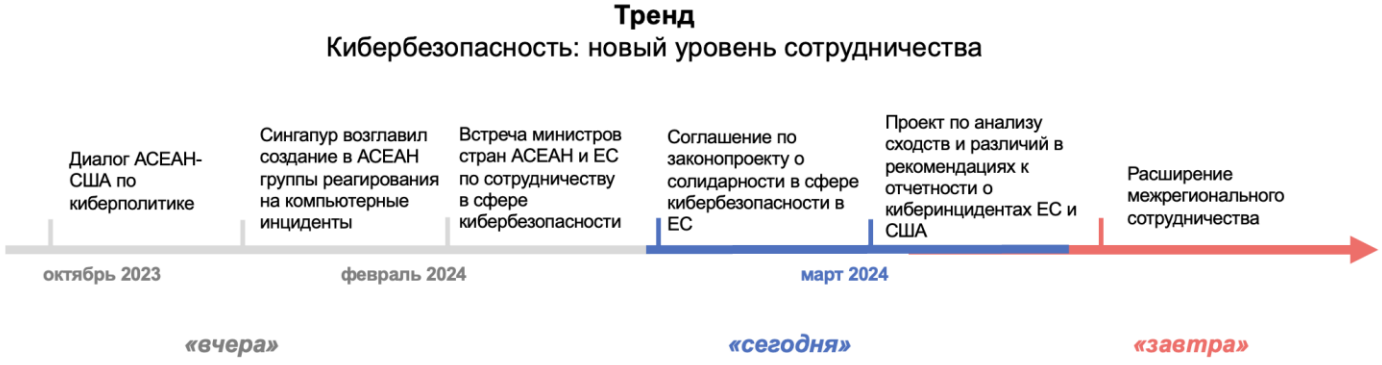
В марте 2024 г. можно выделить 3 события, которые определяют тренды развития регулирования цифровой экономики.

Тренд №1. Борьба с антиконкурентными практиками платформ

В марте 2024 г. в ЕС против платформ Google и Apple началось первое расследование антимонопольных нарушений о несоблюдении Закона о цифровых рынках, который вступил в силу с февраля 2024 г. Например, компании продвигают собственные сервисы на платформах в ущерб аналогичным сервисам конкурентов.

Тренд №2. Кибербезопасность: новый уровень сотрудничества

В марте 2024 г. ЕС сделал важный шаг к принятию закона о создании общеевропейских механизмов реагирования на киберинциденты. Был также анонсирован совместный проект ЕС и США по единым подходам к отчетности о киберинцидентах. В цифровой экономике кибербезопасность создает необходимые базовые условия деловой среды, при этом согласованные подходы позволяют эффективнее противодействовать трансграничным инцидентам. Эти начинания поддерживаются и другими регионами мира: в феврале АСЕАН продвинулась в создании региональной структуры по кибербезопасности.



Тренд №3. Законы для искусственного интеллекта

В марте 2024 г. опубликован Разъясняющий меморандум ОЭСР по обновленному определению системы ИИ, а 13 марта 2024 г. Европарламент одобрил проект Закона об ИИ. Это первый в мире закон, призванный снизить системные риски, бороться с дискриминацией и обеспечить прозрачность ИИ. Выделены 5 категорий ИИ: запрещенные практики ИИ, высокорисковые системы ИИ, ИИ общего назначения, модели ИИ общего назначения с системным риском и системы ИИ, взаимодействующие с физлицами или производящие синтетический контент. Категория высокорисковых систем ИИ также нашла освещение в законопроектах, принятых к рассмотрению в начале этого года в штатах США. Вместе с тем

определения систем ИИ остаются недостаточно ясными, в том числе для разграничения понятий ИИ и умные приборы или привычные модели.

В марте 2024 г. в России также произошло 2 значимых события в сфере регулирования цифровой экономики:

1. Одобрено использование цифровых финансовых активов по внешнеторговым контрактам

В марте 2024 г. принят Закон, разрешающий использовать российские ЦФА и цифровые права для оплаты по внешнеторговым контрактам[1]:

- ПОД/ФТ контроль операций с ЦФА по внешнеторговым контрактам свыше 1 млн руб.;
- признание валютными ценностями ЦФА, включающие денежные требования в иностранной валюте, иностранные ценные бумаги и пр.;
- валютные операции между резидентами и нерезидентами с использованием цифровых прав могут проводиться только по внешнеторговым договорам;
- валютные операции могут проводиться через операторов выпуска цифровых прав и через инвестиционные платформы;
- ЦБ может устанавливать запреты или специальные условия на совершение отдельных видов валютных операций, связанных цифровыми правами;
- резиденты могут проводить такие операции при условии расчетов в рублях.

Такое регулирование, с одной стороны, позволяет расплачиваться ЦФА по внешнеторговым контрактам и частично обходить санкции, с другой – рынок ЦФА довольно маленький (на конец 2023 г. – 350 выпусков ЦФА, 60 млрд руб. обращающихся активов), а также недоступный для иностранных компаний, так как реализовать или продать ЦФА иностранным контрагентам можно только при обращении к российским операторам обмена ЦФА. Разрешение расплачиваться криптовалютами, которые свободно обмениваются за рубежом, дало бы экспортерам большие возможности для снижения санкционного влияния.

Для международной торговли важно также ввести инструменты оплаты в криптовалютах, в отношении которых в России запрещены операции по покупке товаров/услуг. Криптовалюты, в отличие от ЦФА, можно продать на зарубежных биржах, ЦФА – только на российских платформах. Также в России отсутствует регулирование криптобирж и криптообменников, что ограничивает доступ иностранных компаний на рынок России.

2. Предложен законопроект о регулировании маркетплейсов

В марте 2024 г. был предложен законопроект об агрегаторах информации о товарах (как Озон, Вайлдберрис, Яндекс.Маркет)[2]:

[1] https://sozd.duma.gov.ru/bill/1080911-7
[2] https://storage.consultant.ru/site20/202403/06/fz_060324-568223.pdf

1. Регулирование распространяется только на торговлю товарами. С одной стороны, это позволяет исключить из регулирования платформы такси или классифайды (как Авито или Циан), с другой – услуги также являются частью электронной коммерции, где требуется установление гарантий для продавцов (например, от злоупотреблений со стороны платформ);

2. Вводится понятие электронной торговли, которое также ограничено торговлей товарами. При этом понятие «агрегатор информации о товарах» повторяет понятие «агрегатор информации о товарах (услугах)», закрепленное в Законе о защите прав потребителей, что может создавать коллизию при применении норм;

3. Расширено понятие покупателя – это не только потребитель – физическое лицо, но и юридическое лицо, что позволяет охватить регулированием как B2C, так и B2B торговлю;

4. Установлены дополнительные обязательства агрегаторов в части мониторинга торговли товарами, тогда как в практике зарубежных стран чаще всего действует принцип ограничения ответственности маркетплейса за действия третьих лиц на платформе при внедрении комплаенса;

5. Закрепляется специальный статус для агрегатора, который занимает значимое положение на рынке, – на него приходится более 25% сделок. Для такого агрегатора установлены ограничения: не создавать дискриминационных условий, не навязывать контрагенту дополнительные услуги, не запрещать контрагентам работать с другими агрегаторами или не устанавливать паритет цен, не создавать преимущества для собственных товаров/ услуг. Также важным является запрет на введение принудительного снижения цен на товары продавцов. Агрегатор должен уведомлять контрагентов об изменении условий договора, ухудшающих положение, не менее чем за 30 дней.

Помимо этого, установлены обязательные требования к содержанию договора об оказании услуг агрегатором продавцу и владельцу пункта выдачи заказов, процедурам идентификации продавца при регистрации на платформе агрегатора и пр. Установлена обязанность агрегатора по проверке возраста покупателей для ряда категорий товаров, что в дальнейшем позволит запустить торговлю через агрегаторы, например, алкогольной продукцией. Кроме того, установлена обязанность агрегатора обеспечивать соразмерность санкций, налагаемых на продавцов и владельцев пунктов выдачи заказов, что создает гарантии для предпринимателей на платформах от чрезмерных и несправедливых санкций со стороны платформ.

Идея регулирования марктеплейсов была предложена еще в 2021 г. (первые законопроекты). Тем не менее в данном случае важно создать правовые гарантии как для маркетплейсов – с точки зрения снижения ответственности за незаконные действия продавцов (например, размещение запрещённой законодательством информации или нарушение прав интеллектуальной собственности третьих лиц), так и для продавцов – от необоснованных штрафов со стороны маркетплейсов или принудительного участия в распродажах.

Ключевые аспекты

1. Борьба с антиконкурентными практиками платформ

Опыт США, ЕС и Китая

В марте 2024 г. Еврокомиссия начала первое расследование по соблюдению Google и Apple[3] требований Закона о цифровых рынка. Apple обвиняется в ограничении возможности разработчиков свободно продавать свои приложения через сервисы Apple взимает дополнительные сборы и создает технические ограничения, нарушая нормы конкуренции. Google отдает предпочтение собственным сервисам в ущерб сервисам конкурентов.

Еще с 2021 г. Китай, ЕС и США начали борьбу с антиконкурентными практиками платформ. При этом ЕС[4] и США[5] распространяют специальные правила на «крупные платформы», Китай – на любые[6].

Страны устанавливают перечень антиконкурентных практик платформ:

1. Объединять персональные данные, например, для формирования цифрового профиля (только ЕС). Нельзя объединять данные, полученные от услуг соцсети, с данными при оказании рекламных услуг;
2. Предоставлять преимущества собственным продуктам по сравнению с продуктами продавцов на платформе;
3. Создавать более благоприятный режим при рейтинговании для собственных продуктов/услуг по сравнению с аналогичными продуктами/услугами продавцов или конкурентов;
4. Ущемлять в части условий обслуживания одних продавцов по сравнению с другими;
5. Использовать непубличные данные, сгенерированные продавцами при использовании сервисов платформы для конкурирования с таким продавцами;
6. Ограничивать возможность продавцов продавать клиентам продукты/услуги через сторонние платформы или по собственным прямым каналам онлайн-продаж по ценам и на условиях, которые отличаются от тех, что предлагаются через сервисы платформы;
7. Применять связывающие соглашения, т.е. требовать от потребителей использовать одни услуги платформы для доступа к другим услугам.

Кроме того, в ЕС и США у крупных платформ появляется ряд обязательств, например:

1. Обеспечить интероперабельность сервисов платформы с сервисами сторонних поставщиков;
2. Обеспечить потребителям возможность удалять приложения платформы, изменять настройки по умолчанию или использовать приложения других платформ;
3. Обеспечить доступ продавцов к данным, которые генерирует он или его клиенты, а также возможность переноса таких данных.

Опыт России

Статья 10.1 Закона о защите конкуренции устанавливает запрет монополистической деятельности платформой на конкретном товарном рынке, занимающей доминирующее положение, которая:

1) за счет сетевых эффектов оказывает решающее влияние на рынок, где сделки совершаются через платформу, или затрудняет доступ других хозяйствующих субъектов на этот товарный рынок. Но нет методики определения сетевых эффектов;

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689

[4] Регламент 2022/1925, 2022 г. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32022R1925

[5] Законопроект «Американский закон об инновациях и онлайн-выборе», версии 2021 – 2023 гг.

[6] ЕС - на гейткиперов с годовым оборотом от 7,5 млрд евро, 45 млн.потребителей в месяц и 10 тыс. бизнес-пользователями в год; США – на платформы с объемом продаж в 550 млрд долл., 50 млн потребителей и 100 тыс. бизнес-пользователей в месяц. В Китае6 размер платформ не учитывается

2) доля сделок через платформу превышает по стоимости 35% общего объема сделок, совершаемых на этом рынке;

3) выручка за последний год – более 2 млрд рублей;

В отличие от ЕС и США в России оценивается не количество пользователей на платформах, а доля сделок на товарном рынке, проводимых через платформу, что может создавать трудности для определения размера платформы (особенно на мультитоварных платформах) и позиции на рынке.

Разъяснений для платформ о том, какие практики могут запрещаться, нет.

2. Кибербезопасность: новый уровень сотрудничества

Опыт ЕС

5 марта 2024 г. было достигнуто соглашение между Европейским парламентом и Европейским советом по проекту Закона о солидарности в сфере кибербезопасности[7], который предполагает создание:

1) общеевропейской инфраструктуры Центров безопасности – «Европейского киберщита». Состоит из национальных и трансграничных киберцентров, и будет использовать в том числе ИИ для выявления киберугроз и информирования в режиме реального времени лиц;

2) экстренного механизма кибербезопасности для реагирования на киберинциденты. Будет действовать в 3-х областях:

а) координация тестирования в критически важных секторах, включая здравоохранение и энергетику;

б) резерв кибербезопасности ЕС, состоящий из доверенных провайдеров, готовых вмешаться в случае киберинцидентов;

в) финансовая поддержка взаимной помощи.

3) европейского механизма рассмотрения инцидентов в сфере кибербезопасности.

20 марта 2024 г. Европейская комиссия и США анонсировали проект по анализу отчетности о киберинцидентах для согласования трансатлантических подходов по 6 направлениям[8,9]. Цель – реагирование на трансграничные киберинциденты и сокращение затрат мультинациональных компаний на подготовку отчетности.

Опыт АСЕАН

В феврале 2024 г. Агентство по кибербезопасности Сингапура объявило о сотрудничестве со странами – членами АСЕАН по созданию Региональной группы реагирования на компьютерные чрезвычайные ситуации[10].

Опыт России и БРИКС

В России Законом о безопасности критической инфраструктуры предусмотрена система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, создан Национальный координационный центр по компьютерным инцидентам. Центр обменивается информацией о компьютерных инцидентах между «субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты». При этом нет информации о таком взаимодействии со странами ЕАЭС и БРИКС.

---

[7] https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1332.

[8] https://digital-strategy.ec.europa.eu/en/news/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better-align.

[9] 1) определения и пороговые значения для отчетности; 2) сроки, поводы и типы отчетности; 3) содержание отчетов; 4) порядок отчетности; 5) агрегирование данных об инцидентах и 6) раскрытие информации о них.

[10] https://www.csa.gov.sg/News-Events/Press-Releases/2024/singapore-moves-ahead-to-establish-the-asean-regional-cert-to-strengthen-regional-cybersecurity.

3. Законы для искусственного интеллекта

ОЭСР

В марте 2024 г. ОЭСР опубликовала Разъясняющий меморандум по обновленному определению системы ИИ[11].

Прежнее определение системы ИИ[12] модифицировано (с. 4): «Система ИИ – это машинная система, которая для явно или неявно выраженных целей выводит из получаемых ею входных данных, как генерировать выходные данные, такие как прогнозы, контент, рекомендации или решения, которые могут влиять на физическую либо виртуальную среду. Системы ИИ различаются уровнями автономии[13] и адаптивности[14] после введения в действие».

Определение расширяется вместе с развитием практики использования ИИ. Так, ОЭСР сочла системы ИИ, генерирующие контент, настолько значимым видом, что они получили отдельное упоминание в определении, хотя при желании их работу можно рассматривать как последовательность решений по выводу определенных слов/пикселей/звуков. В принципе определение систем ИИ обычно охватывает машинное распознавание объектов и речи, обработку языковой информации, интеллектуальные системы поддержки принятия решений, интеллектуальные роботизированные системы (с. 6, 9).

ОЭСР полагает, что постановку целей для ИИ всегда можно проследить до человека, который инициирует разработку системы ИИ, даже если цели заданы неявно. Однако некоторые системы ИИ могут разрабатывать неявные подцели и ставить цели для других систем.

Опыт ЕС и США

13 марта 2024 г. Европарламент одобрил проект Закона об ИИ[15].

Законопроект[16] выделяет следующие виды ИИ:

1. Запрещенные практики ИИ (8 категорий), например, для создания или расширения систем распознавания лиц с использованием изображений из Интернета либо с камер видеонаблюдения;
2. Разрешенные высокорисковые системы ИИ, например, системы удаленной биометрической идентификации;
3. ИИ общего назначения, среди которого выделяются модели ИИ с системным риском;
4. Определенные системы ИИ (4 категории), взаимодействующие с физическими лицами или производящие синтетический контент, например, генерирующие дипфейки.

Требования к разрешенным видам ИИ различаются в зависимости от их риска: чем он выше, тем большие и более комплексные требования предъявляются: от маркировки до систем управления рисками.

В США законопроекты, направленные на общее регулирование ИИ, в январе 2024 г. были внесены в законодательные собрания Вермонта и Вирджинии[17].

Законодательные инициативы этих штатов США заметно схожи между собой – вплоть до совпадающих формулировок, но есть и базовые различия:

1. Законопроект Вирджинии имеет более узкий перечень лиц, на которых распространяется регулирование, чем в Вермонте: он касается только разработчиков и эксплуатирующих лиц высокорисковых систем ИИ, тогда как в Вермонте предполагаются также нормы,

---

[11] Explanatory memorandum on the updated OECD definition of an AI system. OECD artificial intelligence papers no. 8. March 2024; https://www.oecd-ilibrary.org/docserver/623da898-en.pdf?expires=1710851224&id=id&accname=guest&checksum=E0A20405C7B511BB50F0E6BB10A86556.
Система ИИ – это машинная система, которая способна для заданного набора определенных человеком целей создавать прогнозы, рекомендации или решения, влияющие на реальную либо виртуальную среду. Системы ИИ предназначены для функционирования на различных уровнях автономии.

[13] Автономия системы ИИ при этом означает степень, в которой она может учиться или действовать без участия человека после автоматизации процессов людьми (с. 6).

[14] Адаптивность относится к системам ИИ, которые способны изменять свое поведение после взаимодействия с входными данными и данными после введения в действие (с. 6).

[15] https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law.

[16] https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-13/0138/P9_TA(2024)0138_EN.pdf.

[17] https://legislature.vermont.gov/Documents/2024/Docs/BILLS/H-0710/H-0710%20As%20Introduced.pdf; https://lis.virginia.gov/cgi-bin/legp604.exe?241+ful+HB747H1.

предназначенные для разработчиков систем генеративного ИИ;

2. Законопроект Вермонта является более детальным в части определений и широким в части требований к разработчикам и эксплуатирующим лицам высокорисковых систем ИИ, в частности, в нем прописаны факторы алгоритмической дискриминации, тогда как в Вирджинии дана только отсылка на законодательный запрет;

3. Сфера ответственности в законопроекте Вирджинии по сравнению с Вермонтом сдвинута от разработчиков к эксплуатирующим лицам высокорисковых систем ИИ: например, избежание любого риска алгоритмической дискриминации в Вирджинии предписывается только последним, тогда как в Вермонте обоим.

В части сравнения подходов к регулированию ИИ в ЕС и рассмотренных штатах США можно отметить следующее:

1. Подход к регулированию ИИ в ЕС относительно штатов США:

а) значительно более комплексный: регулирование распространяется не только на высокорисковый и генеративный ИИ (в части, например, дипфейков), но и предъявляет требования к другим типам ИИ;

б) более строгий: определенные практики ИИ (например, распознавание эмоций на рабочих местах) запрещены, независимо от стандартов и требований к системам ИИ.

В принципе распознавание эмоций на рабочих местах может отвечать определению важного решения (сфера занятости) и соответственно попадать в спектр высокорисковых систем ИИ в рассмотренных законопроектах штатов США, если влияет, например, на увольнение при сокращении штата сотрудников, вместе с тем даже в этом случае эксплуатирующее систему ИИ лицо ограничено только обязанностью уведомить работников о функционировании и цели такой системы.

2. В части критериев высокорисковых систем ИИ в целом прослеживается та же тенденция: в ЕС они шире, соответственно режим жестче. Более широкое определение достигается за счет включения в число сфер высокого риска элементов обеспечения безопасности продуктов и безопасности критической инфраструктуры, тогда как в рассмотренных штатах США она касается только определенных интересов людей.

3. Ни одно из рассмотренных определений систем ИИ не является достаточно четким с точки зрения выделения квалифицирующих признаков именно ИИ. Как следствие, сужение предмета регулирования до высокорисковых/несущих определенные риски (например, личному пространству человека) систем ИИ может быть связано с нерешенностью на данный момент задачи четкого отделения ИИ от привычных устройств (например, датчиков температуры на приборах) и созданных человеком моделей (например, эконометрических).

Опыт России

В российском законодательстве ИИ определен, в частности, в Федеральном законе от 24.04.2020 № 123-ФЗ: это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. При этом технологии ИИ включают компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта.

Отметим, что российское определение технологий ИИ в значительной степени пересекается с направлениями применения систем ИИ, перечисленными ОЭСР, вместе с тем само определение ИИ, завязанное на имитацию когнитивных способностей и сопоставление с результатами интеллектуальной деятельности человека, выглядит спорным, поскольку они не измеримы однозначно и различаются между людьми.