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

- **Данные в международной торговле**
- **Антиконкурентные практики онлайн**
- **Защита персональных данных в блокчейне**
- **Подготовка кадров к вызовам ИИ**
- **Рост киберрисков для МСП**

Мониторинг №4 (16) (Апрель 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., юрисконсульт Фонда Экономической политики Голованова Д.А.

«Апрельский дождь прошел впервые,
Но ветер облака унес,
Оставив капли огневые
На голых веточках берез»
С.Я. Маршак

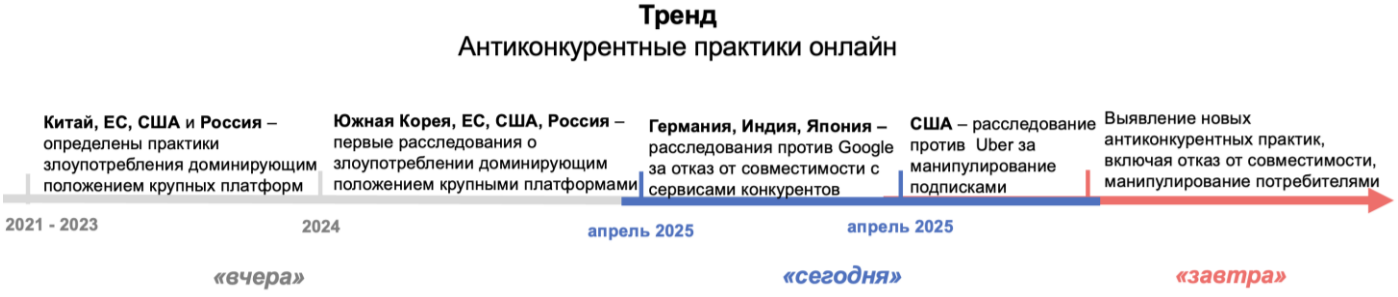
В апреле 2025 г. можно выделить 5 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Данные в международной торговле

В апреле 2025 г. ЕС и Сингапур подписали Соглашение о цифровой торговле по устранению мер, ограничивающих трансграничные потоки данных (как требования к компаниям хранить данные на местных серверах или запрет передавать данные за рубеж), и обмену таможенной информацией для упрощения цифровой торговли.

Тренд № 2. Антиконкурентные практики онлайн

В апреле 2025 г. в Германии завершились расследования против Google из-за злоупотреблений на рынке картографических сервисов, Япония и Индия из-за требований о предустановке сервисов Google на смартфоны и смарт-телевизоры признают отказ от совместимости с сервисами конкурентов антиконкурентной практикой. В США завершилось расследование против Uber за манипулирование онлайн-подписками.

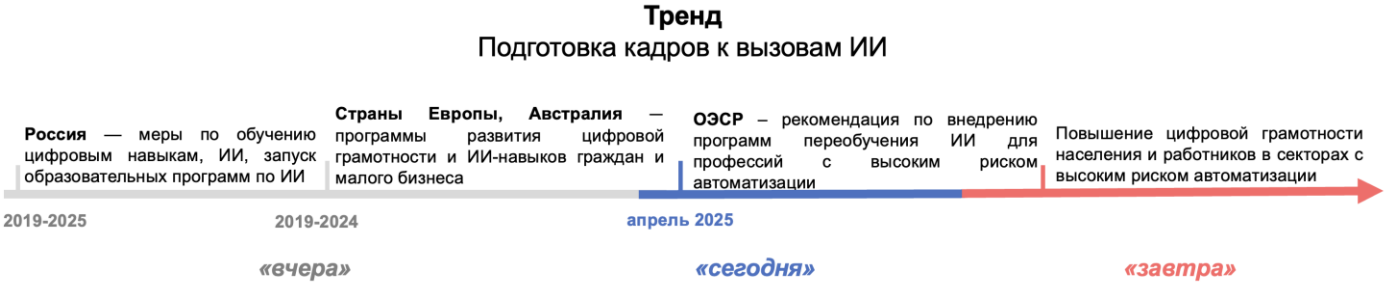


Тренд № 3. Защита персональных данных в блокчейне

В апреле 2025 г. ЕС предложил рекомендации по использованию технологии блокчейн для защиты данных, выделяя риск, что при обработке и хранении данных в блокчейне ограничивается реализация права субъекта персональных данных на удаление и изменение его данных.

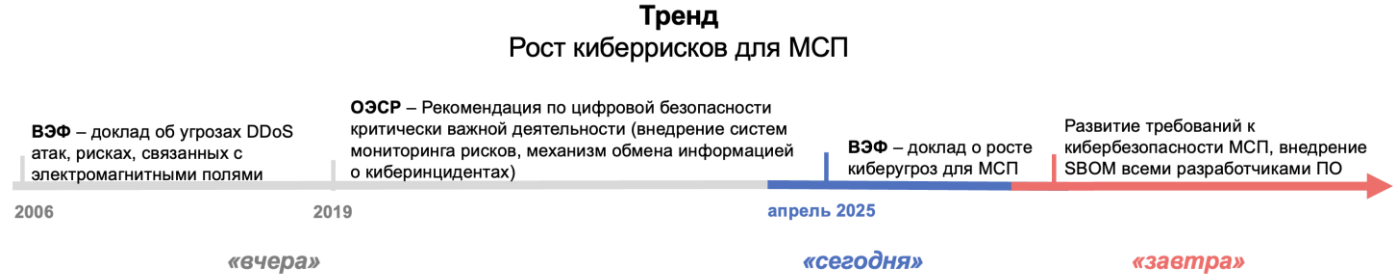
Тренд № 4. Подготовка кадров к вызовам ИИ

В апреле 2025 г. ОЭСР опубликовала доклад о необходимости развития ИИ-грамотности, переобучения работников в связи с ростом автоматизации. Почти треть всех вакансий в странах ОЭСР уже предполагает выполнение задач с применением ИИ, но лишь 1% рабочих мест требует узкоспециализированных ИИ-навыков.



Тренд № 5. Рост киберрисков для МСП

ВЭФ представил доклад Global Cybersecurity Outlook 2025, указав на рост киберрисков для малого и среднего предпринимательства, снижение стоимости кибератак за счет ИИ, а также на проблему развития различных подходов стран к регулированию вопросов кибербезопасности.



В апреле 2025 г. в России введен ряд нововведений.

1. Предложено добирать налог на прибыль с российских транснациональных компаний

В апреле 2025 г. в СМИ со ссылкой на пресс-службу Минфина России появилась информация, что Минфин обсуждает внедрение в налоговое законодательство правила «квалифицированного минимального национального сверхналога» (Qualified Domestic Minimum Top-Up Tax, QDMTT). Правило является частью механизма Pillar 2 ОЭСР[1] в рамках борьбы с размыванием налогооблагаемых баз и выводом прибыли из-под налогообложения. Ранее мы уже описывали механизм Pillar 2 ОЭСР в Мониторинге № 1 (13) (Январь 2025).

Минфин предлагает, чтобы большие транснациональные компании, работающие в России (имеющие дочернюю или материнскую компанию за рубежом), с годовой выручкой не менее 750 млн евро в год платили налог на прибыль в России по ставке не меньше 15%, даже если у них есть льготы. По умолчанию ставка в России – 25%. Однако, например, аккредитованные IT-компании платят только 5% – поэтому компаниям придется доплатить еще 10% с прибыли в России, чтобы достичь уровня 15%.

Уже около 50 стран мира установили у себя правило: если компания платит слишком мало налогов в одной стране, другая страна может сама забрать недостающие деньги (так называемое «правило недообложенной прибыли», Undertaxed Profits Rule, UTPR). Чтобы другие страны не забирали себе налоги с российских компаний, Россия хочет сама добирать налог до 15%. Например, российская IT-компания входит в международную группу с дочерней компанией в Германии и при этом в России она платит только 5% налога (у нее льгота), а «дочка» в Германии – 15%. С новым правилом материнская компания в России будет обязана доплатить еще 10% (чтобы в сумме получилось 15%), а если этого правила не будет, то в Германии (согласно «правилу недообложенной прибыли») налоговые органы получат право взимать с компании дополнительный налог на прибыль, равный тем 10%, что компания не доплатила в России.

[1] https://www.oecd.org/en/topics/sub-issues/global-minimum-tax/global-anti-base-erosion-model-rules-pillar-two.html

Чтобы исключить риск двойного налогообложения, ОЭСР разработала специальный международный отчет по правилам GLoBE[2] (GLoBE Information Return, или GIR). Отчет компания заполняет раз в год и подает в национальный налоговый орган, далее страны обмениваются этими отчетами в рамках двусторонних соглашений. Поэтому, если российская компания подает отчет GIR, Германия увидит, что Россия уже взяла налог с материнской компании 15%. Международная система обмена информацией помогает проверять, правильно ли рассчитан налог.

На глобальном фоне Россия повторяет шаги ЕС, Великобритании, Австралии и Канады, где собственные «сверхналоги» уже утверждены или находятся на финальной стадии рассмотрения. В этих странах льготы постепенно переводятся из формы снижения ставки в субсидии или гранты, которые не учитываются при расчете эффективной ставки GloBE. Минфин России пока не предлагает аналогичных компенсаций.

2. Введены меры противодействия телефонному мошенничеству

Принят новый закон о противодействии мошенничеству с использованием средств связи[3]:

- планируется создать государственную информационную систему, содержащую сведения о мошенниках и данные сотовых номеров, используемых для мошенничества. Система будет доступна только правоохранительным органам, банкам и операторам связи;
- вводятся новые обязательства для кредитных организаций в части ограничений на снятие наличных средств при мошенничестве. Банки должны будут проверять запросы клиентов на снятие наличных по критериям, установленным Банком России (еще не разработаны);
- вводится запрет на использование иностранных мессенджеров при взаимодействии банка с клиентами;
- клиенты банков получают возможность назначить в своем банке уполномоченных лиц (например, кого-либо из родственников) для подтверждения денежных операций с их счетами;
- для защиты потребителей закон наделяет кредитные организации, владельцев агрегаторов (маркетплейсов) правом использования Единой биометрической системы для целей аутентификации своих клиентов или пользователей[4], а микрофинансовые организации обязывает использовать биометрию при выдаче кредитов в дистанционном формате.

Закон вступит в силу 1 июня 2025 г.

3. Утверждены правила признания Роскомнадзором сайта копией заблокированного сайта

Правила[5] приняты во исполнение порядка ограничения доступа к копиям сайтов, на которых неоднократно размещалась запрещенная в России информация (ст. 15.6-1 ФЗ «Об информации»). Выделены признаки сходства копии сайта с непосредственно заблокированным сайтом:

- внешние сходство (как выглядит интерфейс);
- сходство доменных имен, наименований копии, размещенной информации;
- совпадение учетных записей пользователей;
- признаки технического взаимодействия сайта-копии и заблокированного сайта;
- совпадение контактных данных администраторов сайтов.

Перечень не является исчерпывающим, Роскомнадзор вправе блокировать сайт-копию и на основании иных признаков сходств.

---

[2] GLoBE (Global Anti-Base Erosion) – международные налоговые правила, по которым крупные ТНК должны платить не менее 15% налога на прибыль в каждой стране, где они работают.

[3] Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

[4] Ч. 18 ст. 30 ФЗ «О банках», п. 1.4 ст. 9 Закона «О защите прав потребителей».

[5] Постановление Правительства РФ от 16.04.2025 № 493 «Об утверждении Правил принятия мотивированного решения о признании сайта в информационно-телекоммуникационной сети "Интернет" копией заблокированного сайта».

Ключевые аспекты

1. Данные в международной торговле

Опыт ЕС и Сингапура

В апреле 2025 г. подписано Соглашение ЕС и Сингапура о цифровой торговле[6]. Стороны договорились:

1) запретить меры, ограничивающие трансграничную передачу данных. Например, требование использовать оборудование, расположенное только на территории ЕС, без возможности использования оборудования в Сингапуре, или запрет хранения или обработки компаниями ЕС данных на территории Сингапура, и наоборот;

2) гармонизировать режимы защиты персональных данных, учитывая Руководящие принципы ОЭСР[7] по защите неприкосновенности частной жизни и трансграничных потоков персональных данных 1980 г.[8] Руководящие принципы, например, включают стандарт целевого использования данных, т.е. допускается использование данных только в соответствии с целью, на которую дано согласие;

3) развивать открытые правительственные данные, которые могли бы использоваться в производстве товаров и услуг цифровой торговли. Для них устанавливаются критерии: машиночитаемый формат; возможность работы с данными (редактирование, копирование и др.); осуществление доступа к данным через удобный и понятный интерфейс; размещение открытых данных вместе с метаданными; доступ к данным на безвозмездной основе и пр.;

4) развивать системы единого окна для упрощения администрирования цифровой торговли[9]. Предполагается запустить информационный обмен между таможенными органами ЕС и Сингапура, чтобы облегчить движение товаров электронной торговли. Например, обмен таможенной информацией позволяет классифицировать товары по рискам и ускорять процедуры ввоза для товаров с низкими рисками;

5) противодействовать мошенническим практикам против потребителей, таким как реклама товаров и услуг без намерения поставить товары (реклама-приманка).

Опыт России

Россия еще не заключала международные соглашения о цифровой торговле для упрощения трансграничных потоков данных. Однако ЕАЭС работает над несколькими такими соглашениями.

Так, с 2022 г. запущена работа над проектом Соглашения об обороте данных в ЕАЭС[10]. Текста соглашения пока нет, однако в странах ЕАЭС действуют национальные ограничения для оборота данных (как требования локализации в России и Казахстане). Отсутствует гармонизация в режимах защиты данных, например, не гармонизированы требования к формату согласия (в Армении и Беларуси – письменное и электронное, а в России и Казахстане допускается иная форма).

В феврале 2025 г. было утверждено Соглашение ЕАЭС об электронной торговле товарами[11]. Для повышения прозрачности процессов в электронной коммерции в ЕАЭС государства обязуются предоставлять доступ к открытым данным, используемым в сфере взаимной электронной торговли – их перечень утвердит ЕЭК. Устанавливается национальный режим действия законодательства о персональных данных. Однако Соглашение не регулирует проблемы защиты участников электронной торговли, например, не содержит ограничений на недобросовестные коммерческие практики (как введение в заблуждение о цене товара), не регулирует проблемы трансграничных потоков данных.

---

[6] https://data.consilium.europa.eu/doc/document/ST-5854-2025-INIT/en/pdf

[7] Организация экономического сотрудничества и развития.

[8] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[9] Прим.: Единое окно – это информационная система с единым входом для экспортеров и импортеров по взаимодействию с органами различных стран, уполномоченными в сфере регулирования внешнеэкономической деятельности.

[10] https://eec.eaeunion.org/news/v-eaes-pristupili-k-prakticheskoj-rabote-nad-soglasheniem-ob-oborote-dannyh-/

[11] https://www.alta.ru/tamdoc/25r00014/

2. Антиконкурентные практики онлайн

Опыт Германии

В апреле 2025 г. в ответ на жалобы поставщиков картографических сервисов (как TomTom) против Google были вынесены два решения о злоупотреблении доминированием.

Первое решение касается Google Maps[12]. Это не только карты, но и картографические сервисы, как отображение карт (3D обзоры улиц), навигация по маршруту, закрепление и отображение на карте локаций и пр. Такие сервисы сторонние разработчики приложений для Android могут интегрировать в свои приложения – уже интегрированы в более 10 млн сайтах и мобильных приложениях. При этом Google ограничивал комбинирование Google Maps и картографических сервисов конкурентов. Так, разработчикам запрещалось:

1) использовать карты, информацию о местах на карте или иной контент, отличные от предоставляемых Google;

2) использовать сервисы других поставщиков, которые аналогичны или воссоздают функции Google Maps;

3) соединять сервисы Google Maps и сторонние картографические сервисы, если приложение объединяет картографические сервисы разных поставщиков.

Признано, что Google ограничивает совместимость Google Maps и картографических сервисов конкурентов.

Второе разбирательство связано со злоупотреблениями Google на рынке сервисов для бортовых систем автомобилей (экран отображения маршрутов, управление сервисами с помощью жестов, голосовые помощники и пр.). Google продавала производителям автомобилей пакет GAS – набор сервисов Google Maps, Google Play и Google Assistant для авто.

Однако производители могли подключить только полный пакет GAS (все 3 сервиса), сервисы по отдельности подключать нельзя. Например, использовать Google Maps можно только применяя Google Play и Google Assistant.

Единый пакет GAS вынуждает также производителей автомобилей подключать его весь без возможности компоновать сервисы Google с аналогичными сервисами других поставщиков (как TomTom). Кроме того, Google ограничивал функциональную совместимость своих сервисов с сервисами конкурентов, например, голосовой помощник Google Assistant не взаимодействовал со сторонними картографическими сервисами и голосовыми помощниками.

Опыт Японии

В апреле 2025 г. Японская комиссия по добросовестной конкуренции признала, что Google заключал антиконкурентные соглашения с производителями смартфонов на Android и операторами мобильной связи[13]. Соглашения включали условия об обязательной предустановке сервисов Google.

Производители смартфонов на Android и операторы мобильной связи также могли получать часть доходов от поисковой рекламы, если закрепят Google Chrome в качестве браузера по умолчанию и не будут интегрировать поисковые системы других разработчиков.

Теперь Google должен отменить перечисленные условия в соглашениях, разработать внутренние правила для обеспечения соблюдения антимонопольного законодательства.

Опыт Индии

В апреле 2025 г. Комиссия по конкуренции Индии вынесла решение против Google[14] за антиконкурентные соглашения с производителями смарт-телевизоров. Производители, желающие установить магазин приложений Google Play, должны были:

1) предустанавливать полный пакет приложений Google (Google TV Services и YouTube), что, например, продвигало YouTube и усиливало доминирование Google на рынке видеохостингов;

2) не использовать альтернативные версии Android (форки[15]). Это ограничивало

[12] https://www.internationale-kartellkonferenz.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2025/B7-25-22_GMP.pdf?__blob=publicationFile&v=4

[13] https://digitalpolicyalert.org/change/7432-ftc-investigation-into-google-over-alleged-violations-of-antimonopoly-act

[14] https://www.cci.gov.in/antitrust/orders/details/1182/0

[15] Форки – это модифицированные версии операционной системы, созданные на основе исходного кода оригинальной ОС, но с изменениями в интерфейсе, функциях или встроенных сервисах (могут использоваться производителями устройств как альтернатива стандартной версии Android).

возможность производителей разрабатывать и выпускать устройства на измененной операционной системе Android.

С Google подписано мировое соглашение об отмене указанных положений, также Google должна выплатить штраф – около 2,4 млн долл.

Опыт США

В апреле 2025 г. в Калифорнии суд вынес судебный запрет против[16] приложения Uber One для вызова такси и доставки еды. Uber предлагал платную подписку, утверждая, что потребители экономят до 25 долл. в месяц на поездках и доставках по сравнению с теми, у кого нет подписки. Однако было выявлено, что:

1) реальные доказательства экономии 25 долл. в месяц отсутствуют;

2) Uber без предупреждения и без согласия подключал пользователей к платной подписке. Например, на экране оформления заказа пользователю ставился автоматический флажок, что пользователь может сэкономить с бесплатной пробной версией Uber One. И если отменять флажок, было неясно, что отменяется – заказ или подписка. А через 4 недели Uber автоматически подключал к платной подписке с периодическим списыванием средств;

3) за 48 часов до списания платы Uber уведомляет о возможности аннулировать подписку, однако из-за неясных инструкций по отмене подписки пользователи обращались в службу поддержки, которая, однако, задерживала ответы более чем на 48 часов, после чего уже происходило списание.

Опыт России

Сегодня в России ФАС сконцентрирована на регулировании доминирующих маркетплейсов. Например, до конца марта 2025 г. Ozon и Wildberries должны были создать прозрачный механизм скидок для продавцов. По данным СМИ[17], ФАС также должна определить критерии «крупных» платформ и разработать специальные антимонопольные требования к маркетплейсам, например, ограничения для крупных платформ в вопросах приоритетного продвижения собственных товаров, размера инвестиций в скидки и пр.

3. Защита персональных данных в блокчейне

Опыт ЕС

В апреле 2025 г. Европейский совет по защите данных (EDPB) опубликовал проект Руководства по обработке персональных данных с помощью блокчейна[18] для соблюдения GDPR[19]. Блокчейн содержит персональные данные, так как хранит данные участников транзакций (идентификаторы, IP-адреса), данные о суммах криптовалюты, купленных товарах и пр. Хотя данные зашифрованы[20], не исключается их утечка. По данным Defillama, в апреле 2025 г. фиксировалось 8 взломов блокчейн-сетей со стоимостью ущерба – 113 млн долл.[21] Если в результате взлома происходит утечка данных, то идентификаторы лиц[22] в блокчейне могут использоваться злоумышленниками для доступа к данным реальных людей (как паспортные данные, платежная информация и др.).

Технические свойства блокчейна могут создавать риски для выполнения требований GDPR. Данные реплицируются и передаются между участниками одновременно на разные компьютеры в блокчейн-сети, и любое их изменение или удаление будет видно всем участникам. И если транзакция осуществлена, то данные о ней нельзя удалить, только если данные не будут удалены каждым участником цепочки в блокчейне. Это противоречит принципу ограничения хранения данных целями обработки, ограничивает право субъекта данных на удаление и исправление данных.

EDPB предлагает следующие рекомендации по использованию блокчейна:

– использовать частную разрешенную сеть блокчейн. Существуют разные типы

[16] https://www.ftc.gov/system/files/ftc_gov/pdf/uberonecomplaint.pdf
[17] https://www.vedomosti.ru/business/articles/2025/02/26/1094482-fas-pridetsya-vnesti-novie-antimonopolnie-trebovaniya
[18] Блокчейн – это электронная база данных (единая сеть), состоящая из узлов (компьютеров каждого участника сети), которые поддерживают сеть и подтверждают транзакции (например, Ethereum, Ripple, Solana и др.). Блокчейн сеть хранит данные о транзакциях (например, о передаче криптоактивов между участниками) в виде блоков, каждый из которых связан с предыдущим, соединенных в единую цепочку.
[19] GDPR (General Data Protection Regulation) — Общий регламент по защите данных в Европейском союзе.
[20] С помощью специальных ключей шифрования, т.е. определенные буквенно-цифровые символы – и доступ к данным есть только у тех, у кого есть ключ шифрования.
[21] https://defillama.com/hacks
[22] Идентификаторы физических лиц в блокчейн – записи в блокчейн-сети, относящиеся к конкретному пользователю (может содержать такие сведения, как логины, пароли, паспортные данные, платежная информация и т. д.).

блокчейна, например, частный и публичный. В публичном блокчейне (как Bitcoin и Ethereum) каждый участник может видеть и создавать новые блоки. В частном существует единый центральный узел, который дает разрешение на участие другим участникам: только выбранные узлы могут читать или создавать блоки. Поэтому в частном блокчейне субъекты данных защищены от возможного доступа к их данным;

– в блокчейне может храниться только хэш[23], идентифицирующий лицо, все остальные данные могут храниться конфиденциально вне цепочки. И если субъект данных отзывает согласие на обработку данных или хочет, например, изменить данные, то можно удалить хэш участника в отношении отдельных транзакций, тогда данные будет невозможно идентифицировать с конкретным физическим лицом.

EDPB рекомендует контролерам данных (аналогично операторам данных в России) оценивать:

1) будут ли данные в блокчейне содержать персональные данные;

2) обязательно ли использовать блокчейн или возможно применение альтернативных технологий;

3) какой тип блокчейна использовать;

4) будут ли данные храниться в цепи или вне ее.

Опыт России

В России отсутствует специальное регулирование в отношении защиты персональных данных в блокчейне. При этом 152-ФЗ «О персональных данных» (как и GPDR в ЕС) закрепляет обязательство оператора данных (контролера данных в ЕС) по уничтожению или обезличиванию данных по достижении целей их обработки.

Блокчейн активно развивается в России. В апреле 2025 г. Роснано объявила об использовании блокчейна для системы учета и хранения данных о своих интеллектуальных правах на научные разработки[24]. Но необходима нормативная определенность в отношении использования технологии, включая вопросы персональных данных.

4. Подготовка кадров к вызовам ИИ

Опыт ОЭСР

В апреле 2025 г. ОЭСР представила доклад о подготовке кадров и внедрении ИИ-технологий[25]. Около трети вакансий в странах ОЭСР предполагают использование ИИ, и лишь 1% рабочих мест требует узкоспециализированных ИИ-компетенций (как навыки разработки, настройки ИИ-систем: машинное обучение, построение и обучение моделей, работа с большими данными, использование фреймворков[26] (как TensorFlow и PyTorch[27])).

Наибольшему воздействию ИИ подвержены профессии, где более 70% работников имеют высшее образование – руководители, ИТ-специалисты, ученые, бухгалтеры и переводчики. Более 90% из них – трудоспособного возраста[28]. Однако пока отсутствуют данные, свидетельствующие о массовом вытеснении таких работников в результате внедрения ИИ[29]. В целом для большинства работников достаточно базовых знаний и навыков взаимодействия с ИИ («ИИ-грамотности»): умения применять ИИ-инструменты в повседневных задачах, понимать алгоритмы их работы и оценивать риски, связанные с их использованием.

Анализ образовательных программ показал, что в Австралии, Германии, Сингапуре и США только 0,3–5,5% курсов включают модули по ИИ. Основное внимание уделяется подготовке специалистов по разработке ИИ, а программы по развитию общей ИИ-грамотности менее распространены.

---

[23] Хэширование – криптографический процесс шифрования данных – преобразование исходных данных (например, транзакции или сообщения) в строку символов (последовательность символов и букв) по заданному алгоритму. В самом блокчейне уже виден результат шифрования данных – хэш.

[24] https://www.rusnano.com/news/20250421-gruppa-rosnano-rtsis-sozdayut-blokcheyn-infrastrukturu-dlya-ucheta-oborota-intellektualnykh-prav-na-razrabotki/

[25] https://www.oecd.org/en/publications/bridging-the-ai-skills-gap_66d0702e-en.html

[26] Фреймворк – набор готовых инструментов, которые помогают быстро создавать и обучать модели ИИ.

[27] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/who-will-be-the-workers-most-affected-by-ai_fb7fcccd/14dc6f89-en.pdf

[28] https://www.oecd.org/en/publications/who-will-be-the-workers-most-affected-by-ai_14dc6f89-en.html

[29] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/using-ai-in-the-workplace_02d6890a/73d417f9-en.pdf

Можно выделить следующие тенденции в странах ОЭСР:

– формирование базовой цифровой и ИИ-грамотности широкой аудитории. Так, Австрия реализует проект Digital Everywhere: в 2024 г. проведено 3500 мастер-классов по цифровым навыкам (включая ИИ и кибербезопасность);

– содействие внедрению ИИ и цифровых решений для МСП;

– переобучение работников, подверженных риску автоматизации. Сингапур реализует двухдневные курсы по автоматизации, киберрискам и аналитике для низкоквалифицированных работников (в пищевой, текстильной и обрабатывающей промышленности), среди которых преобладают мужчины без высшего образования и мигранты;

– подготовка высококвалифицированных специалистов в ИИ и смежных областях. Великобритания реализует Skills Bootcamps – 16-недельные курсы по ИИ и цифровым технологиям совместно с работодателями.

ОЭСР рекомендует развивать навыки работы с ИИ с помощью следующих мер:

– финансовая поддержка: субсидии, налоговые льготы, ваучеры на обучение и гранты для работодателей, особенно на обучение работников, подверженных риску автоматизации;

– нефинансовые меры: карьерное консультирование, разработка программ подготовки преподавателей, создание партнерств между вузами и бизнесом;

– снижение порогов доступа: упрощение требований к поступающим на курсы ИИ;

– развитие инициатив по общей ИИ-грамотности через специализированные короткие интенсивные курсы;

– интеграция ИИ-обучения в HR-стратегии.

Опыт России

В апреле 2025 г. анализ Rosbalt показал, что минимум 10 млн россиян (кассиры, операторы станков и «белые воротнички» среднего возраста) рискуют оказаться без работы[30]. Например, FixPrice запустили 5800 терминалов самообслуживания, обеспечив оформление около трети всех чеков. Из-за подобной автоматизации в других торговых сетях (Магните и X5) около полумиллиона кассиров могут остаться без работы[31].

В России развиваются бесплатные или частично субсидируемые курсы по цифровизации. До 2030 г. планируют обучить 600 тыс. человек, Минцифры проводит отбор организаций и программ на получение субсидий[32].

5. Рост киберрисков для МСП

В апреле ВЭФ выпустил Global Cybersecurity Outlook 2025[33], выделив 3 проблемы кибербезопасности: (1) рост киберрисков для МСП, (2) рост интереса организованных преступных групп к «рынку» киберпреступлений и снижение стоимости атак за счет ИИ, (3) различия подходов стран к регулированию кибер-безопасности и, как следствие, повышение затрат на соответствие таким требованиям.

Риски киберустойчивости крупных организаций связаны с уязвимостями поставщиков – субъектов МСП. Так считают 54% опрошенных руководителей крупных компаний. Атакуя систему безопасности поставщика – субъекта МСП, злоумышленник может получить доступ ко всей экосистеме крупной организации.

Еще один тренд – развитие сотрудничества киберпреступников с традиционными преступными группировками. Так, более 220 000 человек продали в рабство на «фабриках» онлайн-мошенничества в Юго-Восточной Азии. Такие «фабрики» собирают персональные данные, запускают кампании дезинформации, проводят социальную инженерию (психологическое манипулирование людьми с целью совершения ими определенных действий).

Развитие генеративного ИИ снижает стоимость проведения «успешной» атаки. Преступники в таком случае даже не пытаются взломать IT-инфраструктуру организаций, а используют дипфейки и приемы убеждения сотрудников организаций совершать транзакции в их пользу. Только за

[30] https://www.rosbalt.ru/news/2025-04-26/yaroslav-ignatovskiy-kak-vpishetsya-ii-v-rossiyskuyu-deystvitelnost-5377851
[31] https://companies.rbc.ru/news/NPD5d7jSuo/fix-price-vnedril-bolee-3-200-kass-samoobsluzhivaniya-v-2024-godu/
[32] https://digital.gov.ru/activity/it-obrazovanie/kod-budushhego-ii
[33] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

прошлый год потери частных лиц и компаний от кибермошенничества составили 1 трлн долл., а отдельные экономики потеряли более 3% ВВП.

Подходы к регулированию кибербезопасности стран различаются, создавая барьеры для бизнеса. Например, в странах ОЭСР установлены различные требования к срокам сообщения операторов критической инфраструктуры об киберинцидентах, формируются разные требования к наличию у программных продуктов SBOM[34] и пр.

Стоит отметить, что выделенные в 2025 г. риски кибербезопасности перекликаются с вызовами, которые ВЭФ выделяла с 2022 г. (когда появился первый Global Cybersecurity Outlook). При этом ретроспективный анализ документов ВЭФ с 2006 г. показывает, что некоторые риски за почти 20 лет все же ушли на второй план. Например, угроза DDoS атак еще в 2013 г. относилась к одной из самых существенных, а в 2025 г. ушла на второй план. По опросам ВЭФ, эту проблему называют существенной только 6% опрошенных.

Опыт России

Российский рынок повторяет международные тренды и вызовы, перечисленные в отчете ВЭФ. По данным ГК «Солар» (крупная компания на рынке кибербезопасности), в 2024 г. компания отразила более 1,8 млрд кибератак на информационные системы клиентов, что в 2,4 раза больше[35], чем в 2023 г.[36] Большинство кибератак в России приходится на субъекты МСП – 81% (38% – малый, 43% – средний бизнес)[37].

В России развивается регулирование кибербезопасности. В апреле 2025 г. приняты поправки, устанавливающие обязанность субъектов критической инфраструктуры использовать только отечественное ПО, сведения о котором включены в Единый реестр российских программ для ЭВМ и баз данных, и которое соответствует требованиям о защите информации[38]. К такой критической информационной инфраструктуре относятся информационные системы и сети, работающие в сфере здравоохранения, транспорта, связи, энергетики, банковской сфере, а также в отраслях промышленности[39].

В отличие от стран ОЭСР, в России не внедрены горизонтальные требования ко всем разработчикам ПО, например, о наличии SBOM – такие требования действуют пока только для организаций, получающих лицензию ФСТЭК (в первую очередь для операторов критической информационной инфраструктуры). Требование о наличии SBOM у программных продуктов позволяет лучше оценивать риски взлома ПО.

[34] Software Bill of Materials, машинно-читаемый список всех библиотек, фреймворков, драйверов и иных компонентов, из которых собрано ПО – аналогично этикетке с составом на продуктах питания.
[35] https://rt-solar.ru/analytics/reports/5335/
[36] https://rt-solar.ru/events/news/4991/?utm_source=chatgpt.com
[37] https://innostage-group.ru/press/news/eksperty-innostage-kiberatak-na-sredniy-i-malyy-biznes-v-2024-godu-stanet-sushchestvenno-bolshe/?utm_source=chatgpt.com
[38] Федеральный закон от 07.04.2025 № 58-ФЗ «О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации».
[39] П. 8 ст. 2 Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».