**В С Е О Б Щ А Я К О Н Ф Е Д Е Р А Ц И Я П Р О Ф С О Ю З О В**

**Департамент по вопросам защиты социально-экономических интересов трудящихся**

**О некоторых вопросах внедрения искусственного интеллекта**

В странах региона и мира расширяется цифровизация экономики, внедряется искусственный интеллект (ИИ), который всё чаще признаётся преобразующей силой, коренным образом меняющей отрасли, экономику, общество и жизнь людей. Однако с большой силой приходит и большая ответственность. С момента запуска ChatGPT в конце 2022 г. [количество сообщений о случаях злоупотребления или причинения вреда с помощью ИИ выросло в 20 раз](https://oecd.ai/en/incidents?search_terms=%5B%5D&and_condition=false&from_date=2014-01-01&to_date=2024-12-09&properties_config=%7B%22principles%22:%5B%5D,%22industries%22:%5B%5D,%22harm_types%22:%5B%5D,%22harm_levels%22:%5B%5D,%22harmed_entities%22:%5B%5D%7D&only_threats=false&order_by=date&num_results=20), усиливая риски, особенно в развивающихся странах, где пробелы в инфраструктуре, данных, навыках и законодательстве усугубляют уязвимость.

Как можно использовать потенциал ИИ, снижая при этом связанные с ним риски? В последнем отчёте Всемирного банка [«Глобальные тенденции в управлении ИИ: развивающиеся подходы в странах»](https://documents1.worldbank.org/curated/en/099120224205026271/pdf/P1786161ad76ca0ae1ba3b1558ca4ff88ba.pdf) представлена дорожная карта.

**Сложности данных искусственного интеллекта и их влияние**

Для эффективного функционирования систем ИИ требуются огромные объёмы данных, причём не только числовых и текстовых, но и изображений, аудио, видео и данных с датчиков. Эти разнообразные типы данных имеют решающее значение для точного моделирования ИИ. Однако пробелы в наборах данных, особенно для конкретных сообществ и менее распространённых языков, могут усиливать предубеждения о полезности ИИ.

[Зависимость искусственного интеллекта от огромных наборов данных также вызывает опасения по поводу конфиденциальности и безопасности данных, особенно там, где речь идет о конфиденциальной личной информации.](https://twitter.com/) Сложные модели машинного обучения часто описывают как “черные ящики”, потому что трудно понять, как система приходит к определенному результату. Такая непрозрачность затрудняет исправление ошибок, особенно в секторах с высокими ставками, таких как финансы или предоставление важнейших государственных услуг, таких как общественная безопасность или социальная помощь.

ИИ также оказывает значительное влияние на окружающую среду. Такие задачи, как создание одного изображения с помощью ИИ, потребляют [столько же энергии, сколько зарядка смартфона, а для выполнения одного запроса в ChatGPT требуется почти в 10 раз больше электроэнергии, чем для поиска в Google](https://arxiv.org/pdf/2311.16863). Эти проблемы требуют создания систем управления, которые не только технически надёжны, но и ориентированы на справедливость, прозрачность и экологическую устойчивость.

**Объединение инноваций и регулирования**

Быстрое развитие ИИ привело к глобальному консенсусу: для укрепления доверия к ИИ и обеспечения того, чтобы он приносил пользу всем, не причиняя вреда, необходимо надёжное управление ИИ. Эта идея лежит в основе ключевых документов, таких как [резолюция Генеральной Ассамблеи ООН о надёжном ИИ](https://press.un.org/en/2024/ga12588.doc.htm) и [доклад Консультативного органа ООН по ИИ о *регулировании ИИ на благо человечества*](https://www.un.org/en/ai-advisory-body). В последнем отчёте Всемирного банка по [этой теме](https://documents1.worldbank.org/curated/en/099120224205026271/pdf/P1786161ad76ca0ae1ba3b1558ca4ff88ba.pdf) также подчёркивается острая необходимость в адаптивных и надёжных системах управления, которые обеспечивают этичность, прозрачность и инклюзивность ИИ.

**Ключевые основы ответственного искусственного интеллекта**

Чтобы страны могли извлечь выгоду из искусственного интеллекта, им нужны правильные строительные блоки:

* **Цифровая инфраструктура**: обеспечение надёжного интернета, передовых систем обработки данных и вычислительной мощности.
* **Человеческий капитал**: повышение квалификации работников и создание каналов привлечения талантов с помощью ИИ.
* **Местные экосистемы**: стимулирование инноваций посредством государственно-частного партнёрства и поддерживающей политики.

Политики часто беспокоятся о том, что чрезмерное регулирование зарождающихся экосистем искусственного интеллекта может задушить инновации. Однако надежное управление ИИ и инновации - это не игры с “нулевой суммой”[[1]](#footnote-1) – фактически, управление и регулирование создают равные условия игры, поощряя большее доверие к решениям ИИ и их внедрение, тем самым способствуя инновациям. [Без доверия ИИ не сможет выполнить свои трансформационные обещания, и разрыв в ИИ будет только расти.](https://twitter.com/)

**Инструменты для директивных органов**

Всемирный банк поддерживает страны на всех этапах внедрения ИИ в управление. Поскольку ситуация постоянно меняется, универсального подхода не существует. ВБ описывает четыре инструмента управления, которые страны могут адаптировать к своим уникальным условиям. У каждого из них есть свои плюсы и минусы, которые можно проиллюстрировать на примере конкретных стран:

* **Самоуправление в отрасли**: добровольные этические стандарты ведения бизнеса, такие как те, что разработаны и приняты такими компаниями, как Google и Microsoft, могут формировать практику, но не имеют обязательной силы и [могут способствовать потенциальным рискам «этического отмывания».](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835010)
* **Мягкое право**: необязательные к исполнению принципы и технические стандарты обеспечивают гибкость, но могут не предусматривать чётких прав или обязанностей.
* **«Песочницы» для тестирования нормативных требований**: контролируемые среды позволяют тестировать инновационные подходы к регулированию, но их запуск может быть очень ресурсозатратным.
* **Жесткое законодательство**: обязательные к исполнению нормативные акты, такие как Закон ЕС об искусственном интеллекте или законодательство на уровне отдельных стран, обеспечивают согласованность и правовую определенность, но должны быть адаптированы к местному контексту с учетом имеющихся возможностей и ресурсов.

Страны должны найти баланс между инновациями и мерами безопасности, адаптируя свои подходы в соответствии с имеющимися ресурсами, приоритетами и потребностями общества.

**Почему это так важно**

ИИ — это не только технологии, но и люди. Это создание равных возможностей, защита прав и укрепление доверия. В докладе содержится призыв к политикам действовать смело и сообща, чтобы ИИ стал силой добра.

Следует отметить, что в МПА СНГ в 2023 г. были приняты Рекомендации по нормативному регулированию использования ИИ, включая этические стандарты для исследований и разработок, которые призваны стимулировать разработку и применение систем ИИ в различных отраслях экономики стран Содружества с соблюдением прав граждан и обеспечением безопасности личности, общества и государства. Рассматривается проект модельного закона о регулировании ИИ, разработанный учеными Беларуси.

В ВКП сделана попытка собрать информацию по регулированию искусственного интеллекта и в целом цифровой экономики. Ряд научных организаций стали заниматься этой проблемой. Соответствующий мониторинг ведет Лаборатория анализа лучших международных практик Института экономической политики им. Е.Т.Гайдара, отдельные материалы которой будут приведены далее.

**Ужесточение оборота персональных данных**



В октябре 2024 г. ряд стран и регионов приняли или рассматривали проекты нормативных актов, расширяющие и/или уточняющие обработку персональных данных, в том числе в сфере финансов.

Так, в **США** хотя отсутствует федеральный закон о персональных данных, однако принимаются отраслевые и региональные акты. Так, 22 октября 2024 г. Бюро по правам потребителей в финансовой сфере выпустило правило, требующее от поставщиков финансовых услуг бесплатно передавать персональные финансовые данные другим поставщикам финансовых услуг по запросу потребителя и поддерживать безопасные интерфейсы для направления запросов и получения данных.

Речь идет о праве на переносимость персональных данных. Потребители смогут проще менять поставщиков финансовых услуг на более подходящих (например, с меньшими комиссиями или ставками по кредиту) без неудобств, связанных с потерей данных (истории платежей, регулярных платежах и т.п.). Такие правила ограничат применение «темных» практик, например, сбор персональных данных методом подмены, когда покупатели привлекаются на сайт выгодным предложением несуществующего товара/услуги. Правило будет внедряться последовательно от крупных компаний к меньшим с 01.04.2026 до 01.04.2030.

Кроме того, 1 октября 2024 г. вступил в силу Закон штата Монтана о защите данных потребителей. Физлица – резиденты штата получили ряд привычных для иных юрисдикций (например, ЕС) прав, таких как удаление своих персональных данных, получение их копии для переноса к другому поставщику услуг (например, фотохостингу) и отказ от обработки своих данных в целях таргетированной рекламы или профилирования для принятия автоматизированных решений (например, о доступе к кредитным средствам или медицине).

Контролеры данных теперь обязаны, в частности, ограничить сбор персональных данных, которые необходимы для конкретной цели. Особенностью, характерной для практики США, является прямое регулирование продажи персональных данных контролерами с согласия субъектов данных. В других юрисдикциях, где продажа персональных данных компаниями напрямую не запрещена (например, ЕС), регулирование обычно ограничивается общими принципами обращения персональных данных при отсутствии специальных норм, посвященных продаже данных. Закон Монтаны специальные нормы содержит: не устанавливая ограничений для продажи персональных данных (например, цели продажи и т.п.), кроме согласия субъекта данных, закон относит их продажу к видам обработки данных с повышенным риском причинения вреда субъектам данных, в связи с чем требует проводить и документировать отдельную оценку защиты обрабатываемых для этих целей данных. При этом закон не распространяется на бизнес, обрабатывающий персональные данные менее 50 тыс. субъектов или 25 тыс., если компания получает более 25% доходов от их продажи.

В парламенте **Великобритании** 23 октября 2024 г. был представлен проект Закона об использовании данных и доступе к ним. Ожидается, что наибольшее влияние будет оказано на организации, в том числе международные, в сферах цифровых, исследовательских, медицинских услуг и пр.

**Защита прав работников при использовании искусственного интеллекта**



**США** – одна из первых стран, где планируют урегулировать факт использования ИИ при принятии решений в отношении работников.

В США за последние несколько лет произошел ряд судебных тяжб, связанных с дискриминацией работников в связи с использованием решений систем искусственного интеллекта. Так, в 2022 г. признали нарушение компанией iTutorGroup Закона о возрастной дискриминации: программное обеспечение на основе ИИ для подбора персонала отклонило более 200 кандидатов старшего возраста. В результате компания выплатила $365000 заявителям, которым было отказано по причине возраста. В связи с этим активно развивается регулирование использования ИИ и связанных с ним технологий при принятии решений на рабочем месте.

В феврале 2024 г. соответствующие законопроекты рассматривались в сенатах штатов Нью-Джерси, Нью-Йорка, Массачусетса, Иллинойса. Другие страны пока не выпускали схожее регулирование. Сегодня такие программные продукты, в основе которых лежат машинное обучение, ИИ, анализ больших данных, позволяют принимать решения в отношении трудоустройства работника, а также регулировать трудовые отношения с работниками (повышение, увольнение). Идея состоит в том, чтобы обязать работодателей предупреждать работников или соискателей о применении таких технологий, разъяснять как она работает.

Основные цели регулирования: (1) предотвратить дискриминацию на рабочем месте при использовании технологий ИИ и связанных с ним технологий; (2) обеспечить человеческий контроль над инструментами AED и его решениями; (3) обеспечить доступность всей информации и понимание работы инструментов AED.

Можно выделить следующие направления, которые акцентируются в рамках регулирования: 1) обязательное уведомление кандидата/работника о том, что используется инструмент AED; 2) запрет или ограничение на использование технологий, которые позволяют считывать эмоции или проводить анализ поведения человека; 3) установление человеческого контроля в отношении сгенерированных решений. Так, в Массачусетсе работодатель не может полностью полагаться на решения, сгенерированные инструментом AED, особенно при определении заработной платы сотрудников и принятии решения о найме, продвижении по службе, увольнении или дисциплинарном взыскании; 4) проведение аудита инструментов AED на ежегодной основе. Такой аудит направлен на предотвращение дискриминации работников, включая возраст, расу и пр., и на выявление ошибок, отклонений, нарушений прав работников. 5) введение специального регулирования для работодателей, которые просят соискателей записывать видеоинтервью и проводят анализ таких видеороликов с помощью ИИ, либо используют сервисы распознания лиц.

В странах СНГ в настоящее время отсутствует регулирование ИИ при найме на работу. Хотя в России, например, распространены подобные технологии (например, используется робот-рекрутер «Вера»). В связи с этим можно было рекомендовать дополнить трудовые кодексы государств региона, закрепив право работника или соискателя знать, что работодатель использует автоматизированные инструменты принятия решений на основе ИИ или других аналогичных технологий, установить запрет на использование таких технологий в целях дискриминации работника, либо в целях, не связанных с трудовыми. Также важно проведение аудита автоматизированных технологий.

Следует отметить, что принятая весной 2024 г. Директива ЕС по платформенным занятым вводит новые правила, которые гарантируют, что человек, выполняющий платформенную работу, не может быть уволен или отстранён от работы на основании решения, принятого алгоритмом или автоматизированной системой принятия решений. Вместо этого цифровые платформы должны обеспечивать контроль со стороны человека при принятии важных решений, которые напрямую влияют на людей, выполняющих платформенную работу.

По настоянию ВКП соответствующее положение включено и в проект модельного закона «О платформенной занятости».

**Регулирование дипфейков**



В России в феврале 2024 г. МВД, Минцифры и Роскомнадзор заявили о необходимости более строгого регулирования дипфейк-технологий: включение в перечень отягчающих обстоятельств использование ИИ при совершении преступлений, запрет дипфейков и установление ответственности за незаконный синтез голоса. В США в этом же месяце на федеральном уровне, а также на уровне штатов был выдвинут ряд законопроектов о запрете создания дипфейков от имени госорганов и бизнеса, а также о запрете создания и распространения дипфейка физического лица, имеющего сексуализированный характер, без согласия на это лица.

В соответствии с подходом стран понятие «дипфейк» содержит следующие характеристики:

1) представляют собой имитирование людей (Китай, США, ЕС), а также могут использоваться для создания любых фейковых новостей (Китай);

2) изображения или звуки на самом деле не являются подлинными, например, содержат изображение или голос человека, который говорит или делает то, чего он на самом деле не говорил или не делал;

3) имитация настолько реалистична, что могут показаться разумному человеку правдивыми или подлинными.

При этом, в соответствии с подходом Китая, ЕС и России, дипфейки создаются с помощью ИИ, включая машинное обучение. Законодатели США расширяют подход – дипфейк можно создать не только с помощью ИИ, но и любой другой технологии (например, квантовых вычислений, технологии анализа метаданных) и ПО.

Страны устанавливают следующее регулирование дипфейков:

1. Отдельные виды запретов на дипфейки:

−запрет на использование дипфейков от имени государственных органов или бизнеса в коммерческих целях (США);

−запрет на создание и распространение дипфейков сексуализированного характера, если лицо не дало согласие на создание или распространение таких дипфейков (США);

−запрет на создание и распространение дипфейков, содержащих запрещенный законодательством контент, либо направленных на запрещенную законодательством деятельность (Китай).

2. Устанавливаются специальные права на собственное изображение и голос лица, которое позволяет передавать такие права третьим лицам (Китай, США).

3. Обязательная маркировка дипфейков (ЕС, Китай).

Фото, голос, видео представляют собой персональные данные человека, поэтому в США, ЕС и Китае также применяются соответствующие законы.

В России сегодня предложены следующие подходы к регулированию дипфейков:

1) включение в перечень отягчающих обстоятельств (ст.63 УК РФ) при совершении преступлений использование продуктов ИИ;

2) запрет дипфейков и ответственность за незаконный синтез голоса.

Подход в России состоит в том, чтобы запретить использование дипфейков, тогда как подход ЕС и Китая – в маркировке дипфейков, чтобы пользователь мог отличить дипфейк от достоверной информации. В США вводится запрет на создание сексуализированных дипфейков без согласия лица и дипфейков от имени госорганов, однако при наличии согласия лица дипфейк может быть создан и распространен.

**Минимальный налог для трансграничных компаний**



В **Сингапуре** принят Закон о минимальном налоге с многонациональных компаний (ТНК), который закрепляет ставку подоходного налога в 15% как минимально применимую ко всем МНК. Еще в 2023 г. ОЭСР в рамках борьбы с размыванием налоговых баз международных компаний разработала механизм глобального минимального налога (Global minimum tax, GMT). Цель механизма – гарантировать, что крупные компании облагаются минимальной налоговой ставкой не менее 15% в каждой стране, где ведут деятельность. Это должно снизить практику перемещения прибыли в юрисдикции с низкими налоговыми ставками.

GMT решает проблему снижения налоговых ставок для корпораций в ряде стран, что делается с целью привлечения МНК в налоговую юрисдикцию. Так, в США в 2017 г. ставка подоходного налога для компаний была снижена с 35% до 21% для повышения налоговой привлекательности страны для ТНК. Это ведет к росту конкуренции юрисдикций за налоговые доходы крупных корпораций и создает риск «гонки ко дну» в части налоговых ставок, чему и должен препятствовать GMT.

Новый Закон Сингапура о минимальном налоге для МНК в 15% распространяется на компании, чья совокупная консолидированная выручка по меньшей мере за 2 года из последних 4-х превышает 750 млн евро. Расчет ведется на основе консолидированной финансовой отчетности их конечного материнского предприятия, в которую входят доходы всех предприятий в группе, работающих в стране. Помимо минимальной базовой ставки, налога на доход дочерних структур ТНК устанавлен национальный добавочный налог, который складывается из сумм налогов, подлежащих уплате всеми дочерними и зависимыми компаниями ТНК по ставке в 15% и фактически не уплаченных в полном размере из-за использования более низких ставок.

В Основных направлениях бюджетной, налоговой и таможенно-тарифной политики **Российской Федерации** на 2024 г. и на плановый период 2025 и 2026 гг. Минфин России предусмотрел оценку необходимости внесения изменений в российское налоговое законодательство. Эти изменения направлены на установление минимального уровня налогообложения для российских холдингов, который соответствовал бы глобально принятой ставке GMT в 15%.

**Антиконкурентные практики онлайн**



В октябре 2024 г. в США вынесены решения по расследованию 2 дел против Google за злоупотребление доминирующим положением. В Корее предложено регулировать риски злоупотребления платформ, связанные с несвоевременными расчетами продавцов.

В первом деле генеральные прокуроры всех штатов и Минюст опубликовали заявление о злоупотреблении Google на рынке услуг поисковой текстовой рекламы в США. Поисковая система Google, где рекламодатели тратят до 80 млрд долл. в год, занимает 90% рынка. Google заключала эксклюзивные соглашения с разработчиками браузеров (как Apple, Mozilla), которые должны «по умолчанию» устанавливать в браузерах поисковик Google в обмен на долю доходов от поисковой рекламы Google.

Аналогичные соглашения заключались с производителями устройств на Android (как Samsung) – было запрещено предварительно устанавливать на устройства другие поисковики, кроме Google.

В октябре 2024 г. генпрокуроры штатов предложили меры правовой защиты от влияния монополии Google. Предлагается ограничить Google в заключении таких соглашений.

Второе дело, рассматриваемое в октябре 2024 г. против Google, началось еще в 2020 г., когда Epic Games (разработка игр и развлечений) подала жалобу на Google из-за злоупотребления на рынке. Google заставляла потребителей и разработчиков приложений пользоваться собственным магазином приложений Google Play Store. Также Google подписывала с производителями устройств на Android соглашения о предоставлении Google преференциального режима – производители размещали магазин Google Play на «главном экране» каждого устройства и предустанавливали еще 30 приложений Google на мобильном устройстве каждого пользователя. В обмен производители получали вознаграждения в виде процента продаж от использования пользователями приложений Google. Разработчики приложений не могли продавать приложения и контент напрямую с собственного сайта или из другого магазина приложений – только через Google Play, если хотели иметь доступ к другим сервисам Google (рекламы, поиска, YouTube). Также Google требовала использовать собственный платежный инструмент Google Play Billing для транзакций с потребителями внутри скачанных приложений, облагая транзакции 30%-ной комиссией, что в 10 раз превышает комиссию других платежных решений. В результате в октябре 2024 г. Окружной суд Калифорнии вынес судебный запрет. Google запрещено в течение 3 лет:

− делить доходы от магазина Google Play с производителями на Android как условие предустановки сервисов Google

− ограничивать возможности обновления приложений, которые скачиваются не из Google Play, а из других магазинов или с сайта разработчика;

− ограничивать (в том числе за счет комиссий) использование платежных инструментов, отличных от платежного инструмента Google Play Billing.

Google должна предоставить возможность размещать на Android другие приложения магазинов.

В Южной Корее в октябре 2024 г. предложены поправки в Закон о добросовестных сделках в крупномасштабном розничном бизнесе в части ограничения злоупотреблений со стороны «крупных» платформ при расчетах с продавцами. Предлагается установить, что если крупная платформа управляет платежами при продаже товаров (услуг) продавцов на платформе, либо платежами управляет назначенное платформой финансовое учреждение, то расчеты с поставщиками в результате продаж должны производиться в течение 20 дней с даты подтверждения покупки. Платформы должны размещать не менее 50% выручки от продаж поставщиков на отдельных финансовых счетах или через страхование гарантий платежей, чтобы обеспечить сохранность средств, полученных от покупателей. Таким образом, снижается злоупотребление платформами, связанные с задержкой выплат продавцам.

В России в 2015 г. ФАС проводила расследование (схожее с расследованием в США) против злоупотреблений со стороны Google Play, когда Яндекс пожаловалась, что производители телефонов на Android, отказались от предустановки операционной системы Yandex.Kit. Google ограничивала в соглашениях с производителями возможность предустановки альтернативных приложений.

ФАС признала злоупотреблением практику Google «связывания товаров» (т.е. обязательную предустановку набора сервисов Google при установке Google Play в телефонах с Android). Штраф за несоблюдение предупреждений ФАС составлял 0,5 млн руб. Что касается возможности в России ограничения злоупотреблений платформ путем задержки расчетов с продавцами (практика Кореи), то подобная инициатива может быть включена в законопроекты по регулированию маркетплейсов, либо в законодательство о конкуренции.

Сообщается в порядке информации.

Департамент ВКП по вопросам защиты

социально-экономических интересов трудящихся

1. Игра с нулевой суммой – термин из теории игр, описывающий взаимодействие, при котором выигрыш одного происходит за счет проигрыша другого. [↑](#footnote-ref-1)