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

- Кибербезопасность стала барьером в торговле
- Как AI преобразует рынок труда
- Рекомендации по управлению рисками агентских ИИ
- Можно ли получить заброшенные биткоины через суд?

Мониторинг №5 (29) (Май 2026)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института Гайдара.
Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Солдаткина О.С., науч. сотр. Черновол К.А., науч. сотр. Голованова Д.А.

Кибербарьеры в торговле

Как кибербезопасность стала барьером в торговле

Автор: Иван Ермохин

МСП в ЕС не имеют средств на соблюдение стандартов кибербезопасности

В мае 2026 г. ОЭСР выпустила отчет о том, как стандарты кибербезопасности становятся барьером для международной торговли.

Кибербезопасность – это комплекс технологий и мер, препятствующих несанкционированному доступу к сетям, устройствам, иной цифровой инфраструктуре.

ОЭСР отмечает: разрозненность регулирования кибербезопасности в странах ведет к росту затрат компаний на соблюдение таких требований и снижает сам уровень безопасности инфраструктуры.

Так, затраты европейских компаний на кибербезопасность оцениваются в **31,2 млрд евро** ежегодно. Например, в ЕС с 2023 г. действует Директива о кибербезопасности (NIS2), которая обязывает компании из критически важных секторов системно управлять киберрисками, предотвращать инциденты и быстро сообщать об инцидентах регулятору. Для компаний, которые уже внедряли меры кибербезопасности, рост расходов ожидается на **12%**, а для тех, которые только попали под новое регулирование, – на **22%**.

Сложно не согласиться с основными выводами отчета. Цифровизация отраслей несет скрытые риски: теперь одной кибератаки достаточно, чтобы оставить целый город без электричества, как это уже было в Иране.

Однако отсутствие общих позиций на международном уровне может превращать требования кибербезопасности в то, что ОЭСР называет «бумажной работой»: бизнес занят уже не столько обеспечением безопасности, сколько пытается выполнить все требования. Стоимость такого соблюдения тоже существенна: ОЭСР оценивает в **200–500 тыс. евро** на компанию в ЕС. В России такие затраты оцениваются в **800 тыс. руб.** ежегодно.

34%

Сами по себе требования становятся инструментом торгового протекционизма. Так, ВТО отмечает, что **более 1/3** всех новых торговых споров сегодня затрагивают вопрос кибербезопасности. Поэтому предъявление высоких стандартов кибербезопасности, в том числе через требования сертификации оборудования и ПО, локализацию хранения данных и др., может создать более ощутимые барьеры для входа иностранных компаний, чем прямые ограничения на иностранные инвестиции. При формально открытом рынке для иностранного присутствия стоимость комплаенса для иностранной компании может превышать возможные выгоды от выхода на рынок.

Примечательна, например, серия запретов в отношении компании Huawei на американском и европейском рынках. Ограничения коснулись возможности закупок государственными структурами оборудования китайской компании, а также использования оборудования Huawei для развития 5G сетей. Основанием для ограничения доступа стали именно требования к кибербезопасности, которым компания не соответствовала.

Сам Китай также не отстает во внедрении стандартов кибербезопасности: только в 2018 г. Технический комитет ТС260 выпустил около **300** национальных стандартов кибербезопасности, включая требования к программному обеспечению, маршрутизаторам, коммутаторам и межсетевым экранам. В 2023 г. стандарты были детализированы – вступил в силу дополнительный пакет требований ТС260.

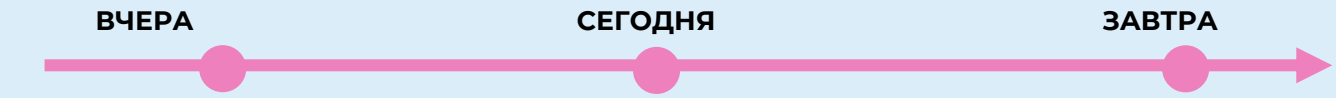
Если говорить о России, то вопрос международного сотрудничества по вопросам кибербезопасности поднимается и на уровне ЕАЭС, однако в основном в контексте информационного взаимодействия в рамках Союза (ст.23 Договора о ЕАЭС) – вопрос выстраивания государственной IT-инфраструктуры для

взаимодействия, а не гармонизации требований к бизнесу.

Снижать издержки компаний на информационную безопасность ОЭСР предлагает за счет разработки общих подходов к регулированию отрасли.

А что дальше?

С ростом цифровизации количество стандартов кибербезопасности и их детализация будут увеличиваться. Страны могут использовать вопрос информационной безопасности как инструмент торгового протекционизма. При этом страны, где уровень развития цифровизации, в частности уровень внедрения ИИ, находится на высоком уровне, могут быть заинтересованы в гармонизации стандартов кибербезопасности. Это будет способствовать дальнейшей экспансии компаний на внешних рынках.



2010-е годы
Принимаются первые комплексные законы о кибербезопасности

2026 г.
Рост требований к кибербезопасности по кругу лиц, детализация и ужесточение

Более **110** стран приняли стандарты кибербезопасности: **78%** стран - по защите персональных данных, а **63%** - правила уведомления об инцидентах

Продолжится рост требований к кибербезопасности, но крупнейшие экономики будут воспринимать требования информационной безопасности как инструмент не только защиты инфраструктуры, но и торговой политики

На замену естественному интеллекту

Как AI преобразует рынок труда: юристы без работы не останутся

Авторы: Ольга Солдаткина, Кирилл Черновол

В мае 2026 г. в Китае суд присудил **260 тыс. юаней** (38,4 тыс. долл.) компенсации работнику, уволенному из-за замещения его рабочих функций ИИ. Технологическая компания в Ханьчжоу попыталась заменить специалиста по контролю качества больших языковых моделей ИИ-системой, предложив ему должность с зарплатой на **40%** ниже. Суд признал увольнение незаконным.

Это дело наглядно демонстрирует конфликт двух точек зрения на роль ИИ в работе: ИИ-энтузиастов, мотивированных оптимизировать расходы на работников с помощью ИИ, и ИИ-скептиков, поддерживающих работников в гонке скиллов с ИИ. Однако, по мнению ОЭСР, подверженность влиянию ИИ в производственных процессах значительно варьируется по секторам и профессиям.

65% *профессий на рынке труда подвержены влиянию ИИ*

Для измерения подверженности ИИ в ближайшие 5-10 лет ОЭСР провела сравнительный анализ компетенций различных профессий со способностями ИИ[1]: чем больше разрыв между способностями ИИ и профессиональными навыками, тем меньше профессия подвержена замене ИИ. И наоборот: если разрыв минимальный, то заменить человека легко.

Впрочем, не все так однозначно, ведь профессия предполагает решение разноплановых задач: одни задачи – такие как обработка данных – можно оптимизировать с помощью ИИ, а другие – такие как коммуникации и организация людей - не решаются без участия человека.

По этой причине юристы и судьи неожиданно попали в группу профессий, наименее подверженных замене ИИ. Хотя эта работа преимущественно аналитическая – то, с чем ИИ справляется лучше всего. Однако необходимость принятия юридически значимых решений делает юристов незаменимыми.

В результате, с учетом профессиональных особенностей, по некоторым оценкам, ИИ полностью может заменить только до **15%** существующих профессий – в основном в сфере администрирования и документооборота. А вот условия осуществления работы изменятся для **50-65%** профессий, особенно в сфере образования, здравоохранения, науки, искусства, СМИ, услуг ремонта и технического сопровождения.

Получается, замене лучше всего поддаются профессии, связанные с работой в стандартизированной среде, но если в профессии появляется творческий элемент или социальная ответственность, то это уже фактор незаменимости человека. А вот вопреки представлениям о незаменимости физического труда следует учитывать фактор роботизации производств: упаковщики продукции, складские комплектовщики или сборщики деталей уже сегодня находятся в зоне риска.

Полный перечень профессий, наиболее и наименее защищенных от конкуренции с ИИ, представлен на специальной платформе ОЭСР.

На российском рынке труда внедрение ИИ может сказаться позитивно. По оценкам Сбера, благодаря роботизации и генеративному ИИ производительность труда может вырасти от **21%** до **32%** к 2032 г.

[1] Сравнение проводится по 9 направлениям человеческой деятельности: 1) коммуникация; 2) социальное взаимодействие; 3) решение проблем; 4) творчество; 5) метакогниция (осмысление мыслительных процессов); 6) знания, обучение и память; 7) видение; 8) оперирование физическими предметами; 9) технический интеллект.

А что дальше?

Если переносить оценки ОЭСР на Россию с опорой на данные Росстата по обследованию рабочей силы, то в «зоне риска», где ИИ или роботы уже уверенно могут делать то, что делает человек, на 2025 г. находится около **2,1** млн человек[1]. Это служащие в сфере обработки информации, учета и другие офисные служащие[2].

Несколько лучше, но все равно критическая ситуация (к настоящему моменту ИИ освоил только 1-2 необходимых для профессии навыка) еще у **9,3 млн человек**: это продавцы, операторы установок, текстильщики, швеи, рабочие пищевой промышленности и т.д.[3] Уборщики, прислуга и «бизнес-специалисты» пока в безопасности, а лучше всего дела обстоят у

Влиянию ИИ были подвержены профессии, связанные с рутинной работой в стандартизированной среде (как бухучет)

ИИ создает новые профессии, связанные с обслуживанием ИИ-систем, и повышает ценность незаменимых специалистов – юристов и врачей

ИИ меняет условия труда большинства профессий, но трудовое законодательство ограничивает полную замену работников ИИ

---

[1] Самыми близкими профессиями к тому, что уже умеет ИИ, ОЭСР считает офисные, производственные профессии, работников приготовления пищи, текстильной, лесной промышленности и продавцов.
По данным обследования рабочей силы Росстата за 2025 г., в России в таких профессиях занято около 11,36 млн человек. Столько работников в профессиях, задачи которых, по мнению ОЭСР, уже может выполнять ИИ.

2 Служащие в сфере обработки числовой информации и учета материальных ценностей – 1 081 451 человек.
Служащие общего профиля и обслуживающие офисную технику – 529 960 человек.
Другие офисные служащие – 487 502 человек.
Сумма всех перечисленных выше работников: 1 081 451 + 529 960 + 487 502 = 2 098 913 человек.

3 Операторы промышленных установок и стационарного оборудования – 1 883 204 человек.
Рабочие пищевой, деревообрабатывающей, текстильной и швейной промышленности и рабочие родственных занятий – 1 641 286 человек.
Сборщики – 427 488 человек.
Помощники в приготовлении пищи – 153 243 человек.
Продавцы – 5 158 606 человек.
Сумма всех перечисленных выше работников:
1 883 204 + 1 641 286 + 427 488 + 153 243 + 5 158 606 = 9 263 827 человек.

ИИ под прикрытием

Первые рекомендации по управлению рисками агентских ИИ

Автор:
Кирилл Черновол

В этом году исполняется 70 лет с момента, когда термин «искусственный интеллект» был принят научным сообществом. Любопытно, что автор термина, Джон Маккарти, умер в том же 2011 г., когда компания Apple запустила голосового помощника Siri.

В мае 2026 г. в странах опубликованы первые меры регулирования агентских ИИ-систем. Почему и что это такое?

Допустим, мы просим ИИ сделать анализ рынка. Генеративный ИИ без дополнительных инструментов возьмет информацию из данных, на которых обучен, составит текст, похожий на «анализ рынка», выдаст его и «забудет» и задачу, и свой ответ. Агентский ИИ – подвид генеративного, способный «разбить» запрос на подзадачи, спланировать, какие данные и откуда взять, проверить себя и выдать более «осмысленный» результат. Такой ИИ сам решает, какие шаги выполнить в рамках задачи, какие данные и приложения использовать.

Возникает вопрос: кто отвечает за ущерб, причиненный агентским ИИ?

Например, агентский ИИ в компании ошибочно заказывает поставку товаров. Может ли компания отказаться от заказа, потому что он сделан без участия человека? Нужно ли установить обязательное одобрение заказа человеком? Этим риски агентского ИИ отличаются от традиционных систем ИИ: человек может потерять контроль над действиями и решениями агентского ИИ из-за его высокой степени автономности, при этом сам агентский ИИ может выходить за рамки своих инструкций и тем самым причинять вред.

Так, в Китае в Позиции Управления киберпространства КНР отмечается, что необходимо законодательно разграничить, какие решения агентский ИИ может принимать только с участием человека, какие – без него, а какие вообще нельзя передавать ИИ.

Аналогично в Сингапуре в Модельном руководстве по управлению агентскими ИИ компаниям рекомендуется до запуска агентского ИИ определить, к каким данным он имеет доступ, может ли только читать или также изменять данные, что он может делать только с одобрения человека, т.е. предоставить минимально необходимый доступ. Например, каждый раз, когда ИИ собирается использовать чувствительные данные, отправлять сообщения, совершать платежи и т.п. Также рекомендуется разрешать ему использовать только определенные API[5], давать доступ к программам или данным лишь на время, не разрешать передавать свои права доступа другим системам ИИ.

56%

разработчиков, применяющих ИИ-агенты в 2025 г., указали на риски безопасности и утечек данных при их использовании

Другая проблема агентских ИИ: как отслеживать ход их работы, если они состоят из нескольких ИИ-систем (особенность ИИ-агентов, что один ИИ может делегировать задачи другим), используют разные инструменты (например, почтовые клиенты, мессенджеры), делегируют задачи ИИ и т.д. Цепочки их действий не всегда видны пользователю: агентский ИИ может выдать цепочку своих действий, но что сделали другие агенты или приложения в цепочке – не видно. КНР предлагает осваивать работу ИИ-агентов на блокчейне, чтобы действия каждого агента были максимально прозрачны.

Органы Австралии, США, Канады, Новой Зеландии и Великобритании по кибербезопасности в Руководстве по

[5] программный интерфейс, который позволяет разным приложениям «общаться» и обмениваться данными друг с другом

внедрению агентских ИИ рекомендуют разработчикам агентских ИИ встраивать в системы специальные журналы взаимодействий между агентами: если один агент передал задачу другому, в журнале должно быть отражено, кому, какие действия совершены, какими инструментами и т.д.

Регуляторы стран также указывают на риски цифровой безопасности, например, когда ИИ удаляет данные из других приложений или перегружает их запросами, и т.д. Пример: инцидент с ИИ-агентом Replit, который в ходе работы целиком удалил базу данных разработчика, создававшего с помощью этого агента приложение. Рекомендуют тестировать, как агентский ИИ ведет себя с доступом к разным внешним программам, создавать ИИ-агентов, отслеживающих, чтобы основной ИИ не вредил, и чтобы ИИ на каждом шаге своей работы «держал в уме» цель, зачем он это делает и т.д.

В России пока не наблюдается инициатив по развитию регулирования агентских ИИ. Однако, например, в законопроект Минцифры по ИИ, можно внести нормы со спецификой рисков агентских ИИ, установив правила для разработчиков по внедрению мер отслеживания действий агентского ИИ и пр.

А что дальше?

Чем агентский ИИ опаснее простого чат-бота? Он может задействовать программы, над которыми у вас нет контроля. Если дать ему доступ, агентский ИИ может случайно удалить вашу почту, «слить» платежные данные, плюс возможны обычные для ИИ «галлюцинации», риски искажений и пр.

На 2025 г. компании в мире используют около **28,6 млн** ИИ-агентов; прогнозируется, что к 2030 г. их будет уже более **2,2 млрд.**

ВЧЕРА — **СЕГОДНЯ** — **ЗАВТРА**

февраль 2026
ОЭСР: отчет об агентских ИИ

май 2026
КНР, Сингапур, Австралия, Великобритания и др.: рекомендации по агентским ИИ

ОЭСР выделяет факторы, повышающие риски агентского ИИ: делегирование задач, уменьшение человеческого надзора, прозрачности и др.

Определение рисков агентских ИИ: удаление, изменение или передача данных без разрешения, передача полномочий другим программам, выход за рамки заданных задач и разрешенных действий

Введение мер безопасности агентских ИИ: вести журналы действий программ, которым поручается выполнение задач; ограничивать передачу прав доступа третьим лицам или другим программам и пр.

Заброшенные биткоины

Можно ли получить заброшенные биткоины через суд?

Авторы: Иван Ермохин, Диана Голованова

В мае 2026 г. аноним под псевдонимом Noah Doe и 2 компании из штата Вайоминг (ABC Company и XYZ Company) подали в Верховный суд штата Нью-Йорк иск о признании права собственности на **39 069** неактивных биткоин-адресов. Истцы утверждали, что с помощью разработанного ими алгоритма выявили адреса, которые не использовались более 5 лет и поэтому, по их мнению, могут считаться заброшенными, в связи с чем просили суд признать за ними право собственности на эти адреса и находящиеся на них биткоины.

Согласно Закону Нью-Йорка о личном имуществе, право на потерянное имущество[1] стоимостью менее **10 долл.** может перейти к нашедшему, если он в течение года предпринимал попытки найти владельца. В качестве доказательств истец указал, что передал в полицию флешки со списками найденных адресов и уведомлял владельцев через сообщения в блокчейне. При этом привлеченный истцом независимый эксперт оценил стоимость каждого адреса менее чем в 10 долл., объяснив это тем, что у истца нет доступа к активам, восстановление стоимости связано с высокой сложностью, а получение стоимости при таком восстановлении не гарантировано, хотя фактически на адресах могут находиться биткоины и на большую сумму.

285 млрд долл.

могут стоить биткоины на заброшенных адресах

Таким образом, истец планирует получить право собственности не на сами биткоины, а только на публичные адреса, которые видны в блокчейне и позволяют, например, получать переводы по такому адресу, но не позволяют вывести с такого адреса криптовалюту (так как для этого требуется приватный ключ). Поэтому спорным является вопрос о том, может ли публичный адрес рассматриваться как найденное имущество, если доступ к биткоинам и возможность распоряжаться ими зависят от наличия не только публичного адреса, но и приватного ключа.

В Нью-Йорке действует еще один закон – Закон о бесхозяйном имуществе, в котором уже есть норма о невостребованной виртуальной валюте: криптовалюта может перейти в собственность штата, если такая криптовалюта удерживается организацией, осуществляющей деятельность с виртуальной валютой (например, биржей), и остается невостребованной в течение 5 лет. Однако и этот закон не совсем подходит к рассматриваемой ситуации, поскольку он регулирует виртуальную валюту, которая находится у посредника (например, у биржи), а в иске речь идет об адресах вообще без посредника.

Отдельный правовой вопрос связан с тем, можно ли иметь право собственности по отдельности на публичный адрес и на приватный ключ. И означает ли право собственности на публичный адрес автоматическое получение права собственности на криптовалюту, которой можно воспользоваться только при наличии приватного ключа? Сегодня законодательство стран на этот вопрос прямо не отвечает.

В российском праве цифровая валюта признается совокупностью электронных данных (цифрового кода или обозначения), которые содержатся в информационной системе, могут приниматься как средство платежа или инвестирования[2]. Поэтому публичный адрес или приватный ключ по отдельности вряд ли можно рассматривать как имущество.

[1] Заброшенным или потерянным считается имущество, которое было оставлено владельцем и затем найдено другим лицом.

[2] Федеральный закон от 31.07.2020 № 259-ФЗ.

А что дальше?

Если суд удовлетворит иск, длительное отсутствие операций с криптоактивом может использоваться как аргумент в пользу его заброшенности, хотя на практике владелец может просто хранить криптовалюту и ждать роста ее стоимости.
При этом без приватного ключа истец все равно не сможет перевести биткоины, но сможет ссылаться на судебное решение, если активы начнут двигаться или попадут на биржу.

Fun fact

В 2013 г. британец случайно выбросил жесткий диск с приватным ключом от биткоинов и затем много лет пытался через суд получить доступ к свалке, где, по его словам, находился этот диск. В январе 2025 г. суд отказал ему, указав, что у иска нет реальных перспектив, а жесткий диск после попадания на полигон стал собственностью городского совета.
Примерно в **600 млн** фунтов стерлингов оцениваются потерянные британцем **8 000 биткоинов**.

ВЧЕРА — **СЕГОДНЯ** — **ЗАВТРА**

до 2026 г.
Появились неактивные биткоин-адреса и без приватного ключа ими нельзя пользоваться

2026 г.
В суде пытаются признать право собственности на неактивные биткоин-адреса как на заброшенное имущество

Часть биткоинов фактически оказалась потерянной: владельцы утратили приватные ключи, перестали использовать адреса или не могут получить доступ к ним

Спорным остается вопрос, что именно можно считать имуществом: публичный адрес, приватный ключ или только криптовалюту в целом (все вместе)

Специальные правила для потерянной криптовалюты: когда ее можно считать утраченной, кто может заявлять права на нее и как отличать потерю доступа от долгосрочного хранения

Новости **в мае 2026 г.**, которые нам показались интересными[1].

- В России в Госдуму внесен законопроект о робототехнике и автономных беспилотных системах. Роботов и беспилотники из перечня Правительства нужно будет регистрировать, оформлять им «цифровой паспорт», передавать в единую госсистему данные об их местоположении и параметрах в реальном времени, а при взаимодействии с человеком - предупреждать, что он общается с роботом.

- Во Вьетнаме Минфин предложил разрешить МСП использовать цифровые активы как обеспечение по банковским кредитам вместо традиционного залога (например, недвижимости). При этом МСП составляют более **98%** предприятий во Вьетнаме, но получают только около **19–20%** общего объема банковских кредитов.

- В России посреднические платформы должны предоставлять преференции платформенным занятым, которые оформили добровольное социальное или медицинское страхование. Установлен минимальный размер преференции – 2,9% от дохода занятого. Например, в форме доплаты, скидки на комиссию платформы и др.

- В Техасе начато расследование в отношении Meta из-за возможного нарушения требований конфиденциальности. Компания разрабатывает для своих ИИ-очков функцию распознавания лиц «Name Tag»: при ее использовании могут автоматически обрабатываться биометрические данные людей, на которых смотрит пользователь, в том числе прохожих. Однако такие лица не давали согласие на обработку своих данных.

[1] С 2025 г. Институт Гайдара разрабатывает цифровую платформу анализа новостей в России и в мире по тематике регулирования цифровой экономики – DIgiReg. Представленные новости отобраны экспертами в том числе на основе анализа данных платформы.

DIGEST