



Топ вопросов по ИИ регулированию

REVERA
25+ years of legal experience

1. Охраняется ли авторским правом контент, созданный искусственным интеллектом (ИИ)?

Авторское право на произведение (креативы, дизайн, исходный код или видео) возникает при наличии творческого вклада человека. Если же такого вклада нет, к примеру, ИИ сгенерировал арт на основании промпта в одно предложение, то данный арт **не охраняется** авторским правом.

Если произведение создано с помощью ИИ, то защита авторским правом возможна, если автор приложил существенные усилия по его созданию, к примеру в следующих случаях:

- ✦ автор предоставил оригинальные вводные данные, к примеру, собственноручно подготовленный арт, который ИИ доработал;
- ✦ автор создал произведение с помощью ИИ после длительной череды промптов;
- ✦ автор создал произведение с помощью ИИ и его существенно доработал вручную;
- ✦ автор создал несколько произведений с помощью ИИ и составил из них общее произведение, к примеру, клип или фильм, составленный из множества более мелких роликов, нарисованных ИИ.

Касательно последнего случая, за эталонный пример можно взять позицию американского Copyright Office, там широко известен случай с комиксами Кристины Каштановой, которые – по мнению Copyright Office – как таковые не обладают достаточным творческим характером, так как сгенерированы с помощью ИИ.¹



Однако объект подлежит охране как сборник, так как он создан творческим трудом г-жи Каштановой: подбор и расположение картинок, а также сопутствующий текст.

Другой пример частичной охраны:

The AI system produced this output:

Prompt
«a young cyborg woman (((roses))) flowers coming out of her head, photorealism, cinematic lighting, hyper realism 8k, hyper detailed.»



Copyright Office предоставил возможность регистрации в реестре авторских прав с пометкой «Registration limited to unaltered human pictorial authorship []», то есть сам чертеж и текст, но не итоговый 3D output.²

Подходы к охране ИИ-контента различаются по юрисдикциям и быстро развиваются, поэтому необходимо регулярно мониторить правовые позиции в ключевых рынках и документировать весь процесс создания: от исходных промптов до финальных правок. Рекомендуется внедрить AI Policy для команды и подрядчиков, которая определит правила использования ИИ и требования к документированию — это станет основой для защиты ваших авторских прав.

2. Кому принадлежит авторское право на ИИ-контент?

Если ИИ-контент охраняется авторским правом с учетом описанного в вопросе 1, то в большинстве юрисдикций автором признаются именно люди, чьим творческим трудом создан контент. Общество пока не дошло до идеи со-авторства с ИИ.

Поэтому права на output могут принадлежать разработчикам ИИ систем или их пользователям. Сегодня этот вопрос решается только с помощью пользовательских соглашений.

Владелец GenAI обычно не рассматривается в качестве владельца прав на контент, созданный с использованием

¹ <https://www.copyright.gov/docs/zarya-of-the-dawn.pdf>

² <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf>

его платформы и отношения с пользователями регулируются в Terms of Use. В большинстве ИИ продуктов, например ChatGPT, Midjourney и т.д., права на output признаются за пользователями.³

3. Можно ли обучать ИИ модель на охраняемых материалах?

В ряде стран действуют исключения, которые позволяют обучать ИИ на общедоступном контенте, если нет прямого запрета владельца данных. К примеру, в ЕС это Text & Data Mining exception, на которую полагаются большинство GenAI. Вместе с тем, владелец информации может запретить использование своей информации, к примеру, через размещение на сайте robots.txt, который в автоматизированном режиме будет запрещать анализ информации через AI.

Однако ситуация не имеет однозначного ответа, в частности границы действия данного исключения и в каком случае оно позволяет использовать данные. Кроме того, большинство крупных порталов прописали в свои политики запрет на использование своих данных для обучения ИИ.

С ростом числа дел, таких как OpenAI v. The New York Times и UMG Recordings v. Suno, в случае интеграции произведений в собственную работу (например, подготовка дизайна сайта или персонажей игры) мы советуем получить лицензию.

4. Законно ли использовать персональные данные сотрудников и кандидатов на вакансии при использовании ИИ?

Прямого запрета нет, но действуют жесткие ограничения GDPR и растущие судебные риски. Использование ИИ в HR не запрещено, однако вы обязаны соблюдать все требования GDPR к обработке персональных данных. Это означает: обязательное информирование кандидатов и сотрудников о том, что их данные обрабатываются

ИИ-системами, своевременное удаление данных после завершения процесса найма, строгий запрет на использование специальных категорий данных (раса, религия, политические взгляды) без явного согласия.

Под вопросом использование AI скрининг инструментов, так в деле Mobley v. Workday, истцы утверждают, что алгоритмы дискриминируют кандидатов старше 40 лет. Решение по этому делу станет важным прецедентом для всей индустрии.

В контексте скрининг инструментов, помните о запрете автоматизированного принятия решений. GDPR запрещает принимать решения о найме, увольнении или продвижении исключительно на основе автоматизированной обработки.

Это означает, что вы не можете просто поставить ИИ-агента и переложить на него ответственность — обязательно должна быть человеческая проверка каждого решения.

При внедрении ИИ в HR проведите DPIA (Data Protection Impact Assessment). Это обязательное требование для систем высокого риска. DPIA поможет выявить и минимизировать риски дискриминации, а также станет вашей защитой в случае регуляторных проверок.

5. На ком лежит ответственность при ошибках ИИ?

По общему правилу, ответственность за ошибки, связанные с использованием ИИ, несет лицо или организация, предоставляющие конечную услугу, использующую ИИ. Например, если ИТ-система Компании X по генерации предсказаний исходя из отпечатка ладони интегрирована с API нейросети (того же ChatGPT) — по общему правилу, ответственность за точность и результаты этой системы перед пользователем несет Компания X, а не OpenAI.

Тем не менее, в соответствии с EU AI Act провайдеры ИИ систем (в том числе высокого риска) могут быть привлечены к ответственности в случае нарушения требований к качеству ИИ системы.

³ <https://openai.com/policies/terms-of-use/>

6. Каковы правовые требования к использованию ИИ в разработке игр?

Использование ИИ в играх регулируется общими нормами, но с важными отраслевыми особенностями.

На ИИ-контент в играх распространяются стандартные требования авторского права, защиты персональных данных и ответственности за контент.

Платформы устанавливают собственные правила для ИИ-контента. Steam требует от разработчиков гарантировать законность ИИ-контента, его соответствие маркетинговым материалам и внедрение механизмов предотвращения создания незаконного контента при генерации в реальном времени. При этом в Adult Only играх генерация ИИ-контента в реальном времени полностью запрещена. Epic Games, PlayStation и Xbox также разработали свои политики, которые необходимо изучать отдельно для каждой платформы.

Практические рекомендации:

- ✦ маркируйте ИИ-контент и документируйте процессы,
- ✦ обязательно указывайте в описании игры использование ИИ для генерации контента,
- ✦ ведите документацию по источникам обучающих данных,
- ✦ внедряйте системы модерации для контента, создаваемого в реальном времени.

Особое внимание уделите защите данных несовершеннолетних игроков — это область повышенного регуляторного внимания.

7. Какие риски несет использование ИИ-контента?

Риски нарушения интеллектуальной собственности. Основная угроза — иски правообладателей за использование их материалов в обучающих датасетах без разрешения. Свежий пример: решение суда по делу Thomson Reuters v. ROSS Intelligence (2025) установило, что обучение ИИ на защищенных авторским правом материалах может составлять прямое нарушение. Дополнительный риск — отсутствие авторских прав на созданный ИИ контент, что делает ваши разработки уязвимыми для копирования конкурентами.

Риски качества услуг и операционные сбои. ИИ-системы могут выдавать неточные результаты, галлюцинации или дискриминационные решения, что ведет к недовольству клиентов и репутационным потерям. Особенно критично для customer service ботов, медицинских приложений и финансовых сервисов. Технические сбои ИИ-систем могут парализовать бизнес-процессы, если нет резервных сценариев работы.

GDPR-риски и утечки данных. Использование ИИ часто связано с обработкой больших объемов персональных данных без четкого правового основания — это прямое нарушение GDPR с штрафами до €20 млн. ИИ-системы также создают новые векторы атак: model inversion attacks могут извлечь обучающие данные, а prompt injection — получить доступ к внутренней информации компании.

Регуляторные риски нового поколения. EU AI Act вводит штрафы до €35 млн за нарушения требований к высокорисковым ИИ-системам. В США растет число отраслевых регуляций на уровне штатов. Компании рискуют оказаться в ситуации, когда их ИИ-системы внезапно попадают под новые требования, которые невозможно выполнить без кардинальной переработки архитектуры.

8. Можно ли использовать ИИ-агентов для ведения продаж и коммуникации с клиентами?

Технически можно, но с обязательным раскрытием факта использования ИИ.

В большинстве юрисдикций нет прямого запрета на использование ИИ-агентов в продажах, однако существует требование честности в коммерческих отношениях. Клиенты должны понимать, что общаются с искусственным интеллектом, а не с человеком. EU AI Act требует четкой маркировки ИИ-контента, а законодательство о защите прав потребителей многих стран запрещает вводящие в заблуждение коммерческие практики.

Обработка персональных данных требует особого внимания. ИИ-агент будет обрабатывать персональные данные клиентов (имена, контакты, предпочтения), что автоматически делает вас субъектом GDPR. Необходимо обновить политику конфиденциальности, указав использование ИИ для обработки данных, обеспечить возможность удаления данных по запросу клиента и ограничить доступ ИИ только необходимой информацией. Особенно важно не допускать обучения ИИ на конфиденциальных данных клиентов без их согласия.

Установите четкие границы полномочий и контроль качества. Определите, какие решения ИИ может принимать самостоятельно (например, назначение встреч), а какие требуют участия человека (подписание контрактов, предоставление скидок). Внедрите систему мониторинга переписки ИИ и escalation процедуры для сложных случаев.

Помните: юридическая ответственность за действия ИИ-агента лежит на вашей компании, поэтому любые обещания или соглашения, которые даст ИИ, могут стать юридически обязывающими.

9. Как себя обезопасить юридически, если я хочу сделать ИИ-модель (агента, ассистента), обучить ее и пустить на рынок как самостоятельный продукт или часть ИТ-продукта?

Полностью исключить риски при таком использовании ИИ-системы сложно. С учетом описанных выше рисков и нашего опыта, рекомендуем, как минимум придерживаться следующих правил:

- Заключить договоры с сотрудниками и подрядчиками, в которых будут описаны правила использования и разработки ИИ-систем и работа с open-source базами (ограничения на copyleft лицензии, обязательная отчетность и так далее),
- Разработать внутренние политики по работе с ИИ и open-source датасетами,
- Разработать и опубликовать EULA (пользовательское соглашение) и распределить риски с пользователями в зависимости от юрисдикции бизнеса,
- Нанять DPO для аудита соблюдения норм по персональным данным,
- Проводить промежуточный юридический аудит для проверки «чистоты» прав на ИТ-продукты и соблюдения регуляторных требований в сфере ИИ.

И помните, ИИ - это не только мощный инструмент для развития бизнеса, но и серьезный юридический вызов для тех, кто строит бизнес прозрачно и на долгосрочную перспективу.

Более подробную информацию о запуске AI-Powered стартапа читайте в нашем специализированном гайде.

Если у вас остались другие вопросы в сфере ИИ — команда REVERA готова помочь вам!

