

Справочная
публикация из серии
“ИС и передовые
технологии”


Генеративный ИИ через призму интеллектуальной собственности



WIPO

Многие компании и организации в спешном порядке внедряют инструменты на основе генеративного искусственного интеллекта (ИИ) для создания контента. Такие инструменты предоставляют как значительные возможности с точки зрения содействия операционной деятельности, так и представляют собой серьезный правовой риск из-за существующих неопределенностей, в том числе в области прав интеллектуальной собственности (ИС).

Многие организации стремятся внедрить некие руководящие принципы, чтобы помочь своим сотрудникам снизить возможные риски. Каждая деловая ситуация и правовой контекст по-своему уникальны, однако приведенные ниже руководящие принципы и контрольный список призваны помочь организациям взвешивать риски в области ИС, задавать правильные вопросы и предусматривать потенциальные защитные механизмы.

 **Генеративный ИИ порождает множество рисков и вопросов. Предприятиям и организациям следует задуматься о внедрении соответствующей политики и обучении сотрудников возможностям и ограничениям этой технологии. Такой дальновидный подход крайне важен для того, чтобы избежать проблем, связанных с использованием генеративного ИИ.**

Что представляет собой генеративный ИИ?

Инструменты генеративного ИИ могут создавать новый контент, такой как текст, компьютерный код, изображения, аудио, звук и видео, в ответ на запрос пользователя, который может представлять собой, например, короткое письменное описание желаемого результата. В настоящее время примерами инструментов генеративного ИИ могут служить ChatGPT, Midjourney, Copilot и Firefly.

В основе технологии генеративного ИИ лежит машинное обучение, и инструменты генеративного ИИ обучаются на огромных объемах данных, часто включающих миллиарды страниц текста или изображений. В зависимости от подхода разработчика инструмента ИИ наборы обучающих данных могут состоять из свободно доступной, необремененной информации (чистые данные), защищенных данных (например, произведений, охраняемых авторским правом) или сочетания того и другого.



Обученный искусственный интеллект получает от человека вводные данные, которые запускают сложный цикл, состоящий из миллиардов вычислений, определяющих результат. Как правило, невозможно предсказать результат или определить, влияют ли определенные части обучающих данных на результат и в какой степени.

Обзор проблем

Разработка генеративного ИИ может быть чрезвычайно дорогостоящим проектом, стоимость которого может достигать десятков миллионов долларов США, поэтому большинство компаний и организаций предпочитают использовать инструменты генеративного ИИ сторонних производителей или дорабатывать такие модели на основе собственных данных. Существует следующие общие проблемы и бизнес-риски:

Определение ситуаций использования

Генеративный ИИ может выполнять множество задач, и оптимальные сценарии его использования все еще не определены, в разных компаниях и организациях они будут разными.

Различия в контрактных условиях

Инструменты на основе генеративного ИИ появились совсем недавно, передовой опыт и нормы составления коммерческих условий контрактов пока что еще не сформировались. Условия, на которых разработчики лицензируют свои инструменты ИИ, могут существенно различаться, это включает такие вопросы, как подход к коммерческой тайне и другой конфиденциальной информации, право собственности на результаты, наличие компенсаций, а также обязательства пользователей по снижению рисков путем осуществления мониторинга за действиями сотрудников и их обучение.

Проблемы, касающиеся обучающих данных

Некоторые инструменты генеративного ИИ были обучены с использованием материалов, взятых из Интернета, включая материалы, охраняемые авторским правом, личную информацию, биометрические данные, а также вредоносный и незаконный контент. В настоящее время ведутся судебные разбирательства по вопросу о том, не нарушают ли процессы извлечения, загрузки и обработки материалов в рамках обучения моделей ИИ и генерируемых ими результатов права интеллектуальной собственности, неприкосновенность частной жизни и контрактные обязательства. По сей день продолжаются споры относительно баланса интересов владельцев ИС и разработчиков ИИ.

Проблемы, касающиеся результатов использования ИИ

Генеративный ИИ может генерировать неприемлемые результаты или результаты, нарушающие закон, это включает в себя неверную информацию, нарушения прав интеллектуальной собственности, «дипфейки» (deepfakes), персональные данные, клеветнические утверждения, а также дискриминационный, предвзятый и вредный контент. В настоящее время разрабатываются технические средства защиты, но, учитывая сложность соответствующих вычислений, предсказать поведение ИИ во всех обстоятельствах довольно сложно. Кроме того, законы об ИС в большинстве стран были написаны до появления технологии ИИ, что является причиной неопределенности в вопросе прав собственности на результаты ИИ.

Изменение нормативно-правовой базы

Правительства и регулирующие органы в настоящее время рассматривают возможность внесения новых законов, нормативных актов, политики и руководящих принципов в отношении генеративного ИИ. В результате для предприятий и организаций, использующих генеративный ИИ, могут быть введены определенные требования. Особые правила уже действуют в Китае, а Европейский союз намерен ввести соответствующие нормативно-правовые нормы уже в ближайшее время.

Представленный список проблем не является исчерпывающим, и потенциально существует множество других проблем, например высокий расход электроэнергии на обучение и использование генеративного ИИ.

Многие международные организации, такие как ЮНЕСКО, ОЭСР и Глобальное партнерство по ИИ (Global Partnership on AI), опубликовали свои руководства по общим принципам ответственного использования ИИ. Предприятиям и организациям следует рассмотреть возможность внедрения соответствующей политики и обучения персонала в области генеративного ИИ, чтобы поощрять ответственный подход к его экспериментальному использованию и практическому применению.

Взаимосвязь между генеративным ИИ и ИС

Генеративный ИИ имеет множество точек соприкосновения с ИС и соответствующих неопределенностей. Хотя полностью устранить данные связанные с ИС риски невозможно, нижеследующие соображения могут оказаться полезными для понимания касающейся ИС специфики вопроса в этой развивающейся технической области.

Конфиденциальная информация

Конфиденциальная информация — это информация, которая не является общедоступной, она может как иметь, так и не иметь коммерческой ценности, передается конфиденциально и в разумной степени защищается. Это понятие включает коммерческую тайну, которая представляет собой вид конфиденциальной информации, имеющей (потенциальную) экономическую ценность или обеспечивающей конкурентное преимущество в силу своего секретного характера.



Предприятия и организации, использующие инструменты генеративного ИИ, могут непреднамеренно выдать коммерческие тайны или раскрыть конфиденциальную составляющую коммерчески важной информации в случае, если она используется для обучения или формулирования запроса для инструментов ИИ. Для предотвращения этого им следует предусмотреть наличие сочетания технических, юридических и практических мер защиты.

Риски

Генеративные инструменты ИИ могут сохранять запросы пользователей и обучаться на их основе. Если пользователи используют конфиденциальную информацию при формулировании своего запроса, конфиденциальность может быть утрачена, поскольку поставщик технологии ИИ имеет копию этой информации, кроме того, эта информация может стать частью модели ИИ, и результаты на ее основе будут публичным образом переданы другим пользователям.

Когда компании и организации разрабатывают инструменты генеративного ИИ с нуля или дорабатывают уже существующие инструменты, используя для этого свою конфиденциальную информацию, существует риск того, что она станет достоянием общественности.

Хакеры могут получить обучающие данные, включая конфиденциальную информацию, используя такие приемы, как атака в форме внедрения запроса (prompt injection).

Меры по их снижению

Для того чтобы свести к минимуму риск того, что поставщик технологии ИИ может сохранять ваши запросы или использовать их для целей обучения, проверьте настройки соответствующих инструментов генеративного ИИ.

Рассмотрите возможность использования таких инструментов генеративного ИИ, которые работают и хранятся в частной облачной среде.

Проверьте, будут ли поставщики инструмента искусственного интеллекта хранить, отслеживать и просматривать ваши запросы. Добивайтесь от поставщика предоставления соответствующей защиты и гарантий в отношении любой конфиденциальной информации.

Ограничьте доступ к инструментам генеративного ИИ, использующим конфиденциальную информацию, предоставляя его только сотрудникам, имеющим право доступа к такой информации.




Поставщики частных инструментов генеративного ИИ могут отслеживать и хранить запросы, чтобы проверять их на предмет неправомерного использования. В некоторых случаях запросы могут быть проанализированы сотрудниками поставщика услуг.

Внедрите соответствующую политику для сотрудников и проведите обучение по теме рисков, связанных с использованием конфиденциальной информации для целей формулирования запросов.

Рассмотрите возможность того, чтобы инструменты генеративного ИИ проверялись и контролировались специалистами по информационной безопасности.

Нарушение прав ИС

Обучение многих инструментов генеративного ИИ проводится на основе огромного количества объектов (иногда речь идет о миллиардах единиц), охраняемых ИС. В настоящее время ведется несколько судебных споров, в основе которых лежит утверждение, что сбор и использование таких материалов для обучения ИИ, соответствующие обученные модели ИИ и результаты их работы являются нарушением прав ИИ. Данные судебные разбирательства в основном посвящены авторскому праву и товарным знакам, однако теоретически в них могут быть затронуты и другие виды прав ИС, такие как промышленные образцы, права на базы данных и запатентованные изобретения.

 Существует значительная правовая неопределенность в вопросе о том, являются ли инструменты ИИ, их обучение, использование и результаты их работы нарушением прав ИС. Ответ на этот вопрос может зависеть от юрисдикции. Предприятиям и организациям следует задуматься о снижении риска путем использования не нарушающих права ИС инструментов, получения компенсаций, когда это возможно, проверки наборов данных и внедрения технических и практических мер по снижению вероятности нарушения прав.

Риски

В настоящее время по всему миру ведутся судебные разбирательства по вопросу о том, является ли обучение искусственного интеллекта с использованием объектов, охраняемых ИС, использование таких обученных моделей ИИ и генерируемых ими результатов нарушением прав ИС.

С указанным риском сталкиваются не только разработчики ИИ, но и, потенциально, пользователи инструментов генеративного ИИ. Во многих странах ответственность за различные формы нарушения прав ИС, такие как создание копии произведения, охраняемого авторским правом, не зависит от намерений или осведомленности предполагаемого нарушителя.

Судам еще предстоит определить, могут ли разработчики, поставщики, заказчики и пользователи генеративного ИИ нести ответственность за нарушение прав ИС, выплачивать компенсацию и уничтожать нарушающие права модели или результаты. В настоящий момент не ясно, сочтут ли суды соразмерным вынесение постановлений, запрещающих использование модели ИИ, обученной на охраняемых правами ИС объектах.


Меры по их снижению

Рассмотрите возможность использования таких инструментов генеративного ИИ, которые были обучены исключительно на основе лицензированных, общедоступных данных или ваших собственных обучающих данных.

Выбирая инструмент искусственного интеллекта, обратите внимание на то, готовы ли поставщики того или иного решения предложить гарантии защиты от нарушения прав ИС, в частности авторских прав. Оцените охват и целесообразность возмещения убытков. Например, такая защита может быть ограничена компенсацией для третьих лиц и обусловлена соблюдением договорных ограничений и реализацией мер по снижению рисков.

Тщательно проверяйте наборы данных при обучении или тонкой настройке инструментов генеративного ИИ. Проверяйте наличие прав собственности на ИС, лицензионное покрытие для целей обучения ИИ и соответствие лицензиям корпорации Creative Commons или статусу общественного достояния. Убедитесь в том, что в предполагаемой юрисдикции действуют соответствующие исключения из авторского права.





Что касается потенциальных нарушений авторских прав, то в законах об ИС некоторых стран предусмотрены исключения, которые могут применяться к генеративному ИИ, они, к примеру, могут охватывать такие действия, как добросовестное использование, поиск текста и данных, а также временное копирование. Однако отсутствие согласованности между странами и пока что не проанализированная практика применения этих исключений в отношении генеративного ИИ вносит неопределенность.

Даже в тех случаях, когда суды уже вынесли определенные постановления, принятое решение могло зависеть от конкретных обстоятельств дела, а также от положений национального законодательства.

Следует иметь в виду, что регулирующие органы рассматривают возможность введения обязательств по раскрытию информации об объектах, охраняемых правами ИС, которые были использованы для обучения моделей. Задумайтесь о том, чтобы документировать то, как проходило обучение модели ИИ.


Внедрите соответствующую политику для сотрудников и проведите их обучение, чтобы свести к минимуму риск генерирования нарушающих права ИС результатов. Посоветуйте персоналу не использовать запросы, в которых упоминаются названия сторонних компаний, товарные знаки, охраняемые авторским правом произведения или конкретные авторы/представители творческого сектора.

Рассмотрите возможность внедрения мер по проверке результатов работы ИИ на наличие нарушений перед их использованием. Это может быть реализовано посредством проверок на плагиат, поиска изображений и подтверждения «чистоты» материалов.

Оцените меры по снижению рисков, связанные с ними затраты и операционные риски с учетом контекста.

Обязательства, касающиеся открытого исходного кода

На код, созданный ИИ, могут распространяться обязательства, касающиеся открытого исходного кода. Когда программное обеспечение или код имеют открытый исходный код, это означает, что исходный код находится в открытом доступе, а пользователям часто предоставляются определенные права и свобода на использование, изменение и распространение данного программного обеспечения. Однако эти права и такая свобода сопровождаются обязательствами, которых должны придерживаться пользователи, например указывая авторство, и эти обязательства зависят от конкретной лицензии на программное обеспечение с открытым исходным кодом.

 **Предприятиям и организациям следует задуматься о применимости данного риска к их коду, изучить возможные компенсации и принять технические и практические меры для снижения вероятности возникновения обязательств, касающихся открытого исходного кода.**

Риски

Обучение генеративного ИИ может быть реализовано на основе кода, подпадающего под требования открытого исходного кода, что потенциально может привести к нарушению обязательств, касающихся ограничений на коммерческое использование или авторство. В США по данному вопросу продолжают правовые прения.

Меры по их снижению

Рассмотрите возможность приобретения инструментов генеративного ИИ у поставщиков, реализующих обучение модели исключительно на лицензионных примерах, или внедрения технических мер защиты, таких как обнаружение соответствующих лицензий объектов с открытым исходным кодом.

Рассмотрите возможность приобретения инструментов генеративного ИИ у поставщиков, предлагающих гарантии от нарушения обязательств, касающихся открытого исходного кода. Проверяйте охват и целесообразность применимых гарантий и условий.


В некоторых лицензиях для открытого исходного кода указано, что любой код, который включает открытый исходный код, должен отвечать требованиям той же лицензии для открытого исходного кода. Таким образом, пользователи, интегрирующие сгенерированный ИИ код, могут непреднамеренно внести в свои проекты обязательства, касающиеся открытого исходного кода.

При обучении или детальной доработке инструментов генеративного ИИ тщательно проверяйте обучающие данные на предмет наличия в достаточной мере разрешительных лицензий.

К использованию генеративного ИИ для целей написания кода применяйте подход на основе баланса риска и выгоды. Если обеспечение свободы кода от обязательств, касающихся открытого исходного кода, является критически важным, рассмотрите возможность запретить поставщикам и сотрудникам использовать генеративный ИИ в таких проектах.

«Дипфейки»: права в вопросе внешнего сходства и голоса

Внешнее сходство и голос охраняются во многих странах, однако в подходах к такой охране нет единообразия. Охрана может осуществляться посредством некоторых видов прав ИС (например, если речь идет о коммерции по чужим именам), законов о недобросовестной конкуренции, прав человека, конституционных прав и прав на публичность.

 Генеративный ИИ способен имитировать образ или голос конкретных людей, а некоторые инструменты были специально разработаны для этой цели. Предприятиям и организациям следует учитывать риски, связанные с такими возможностями.

Риски

Несанкционированное использование или имитация чьего-либо голоса или образа может привести к нарушению прав ИС или других прав, при этом возникают сложности, вызванные несогласованностью правовых баз в различных юрисдикциях.

Подражание образу и голосу также может быть чревато репутационным ущербом или судебным иском, например по обвинению в мошенничестве или диффамации. Во многих странах в настоящее время рассматривается возможность принятия специальных законов и правил для борьбы с «дипфейками». Например, в Китае уже приняты нормативные акты в отношении так называемого глубокого синтеза (Deep Synthesis).

Меры по их снижению


Учредите политику для сотрудников и проведите обучение, четко ограничив использование инструментов генеративного ИИ по технологии «дипфейк». Для одобренных инструментов генеративного ИИ обеспечьте исполнение правил, запрещающих упоминать в запросах конкретных лиц.

В случаях, когда синтезировать чей-либо голос или образ необходимо по законной деловой причине, получите необходимое согласие и лицензию от соответствующего субъекта.



Права ИС в результатах работы ИИ и право собственности на них

Неясно, может ли новый контент, созданный инструментами ИИ, такой как текст, изображения или другие творческие материалы, охраняться правами ИС, и если да, то кому принадлежат эти права. Даже если результаты работы ИИ не подлежат охране ИС, их использование может регулироваться условиями договора.

 На вопрос о существовании и принадлежности прав ИС на результаты работы генеративного ИИ четкого ответа нет. Предприятиям и организациям следует добиваться ясности в контрактах в отношении прав собственности и рассматривать возможность использования генеративного ИИ только в тех случаях, когда вопрос права собственности на ИС в результатах работы ИИ не имеет решающего значения для их бизнес-модели.

Риски

В большинстве стран законы в области ИС были написаны без учета фактора генеративного ИИ, что является причиной неопределенности в вопросе о том, может ли в результатах работы ИИ быть ИС и кому принадлежали бы соответствующие права. Это может не создавать проблем применительно к некоторым правам ИС, например товарным знакам, однако в отношении авторского права данный вопрос вызывает широкую озабоченность.

Подаваемые в последнее время патентные заявки, в которых в качестве изобретателя указывается система искусственного интеллекта DABUS, на постоянной основе отклоняются в тех странах, которые выносили по ним решение, поскольку не был установлен изобретатель-человек. На данный момент пока неясно, может ли генеративный ИИ создавать изобретения без участия изобретателей-людей и могут ли такие изобретения быть запатентованы.

Ведомство по авторскому праву США выпустило руководящие рекомендации по регистрации произведений, содержащих созданные ИИ материалы, указав, что для этого требуется творческий вклад человека. Решения данного ведомства дают основания

Меры по их снижению

Изучите условия использования инструментов генеративного ИИ, чтобы понять, кому принадлежит права на ИС (если таковые имеются) в результатах его работы.

Изучите возможности усиления контроля или более четкого установления прав на результаты работы ИИ путем внедрения элементов ИС, таких как фирменные наименования и логотипы, или привлечения человека к творческой модификации или созданию новых вариантов полученных результатов.

Документально фиксируйте роль человека в процессе изобретения или создания объекта.

При наличии такой возможности заключайте договоры, регулирующие то, кому принадлежат авторские права на произведения, созданные компьютером. В разных странах могут быть разные юридические критерии, они могут быть сложны в применении, поэтому подписание договора вносит определенность в данном вопросе.

При заказе произведений требуйте гарантии того, что для их создания генеративный ИИ не использовался.

полагать, что текстовый запрос пользователя сам по себе не может служить основанием для установления авторских прав, поскольку запрос лишь «влияет» на результат. Однако недавно пекинский суд по делам, касающимся Интернета, постановил, что пользователь владеет авторскими правами на изображение, созданное ИИ, поскольку запрос и его параметры формулируются им таким образом, чтобы изображение отражало его эстетический выбор и видение. Эти различные толкования авторского права на произведения, созданные ИИ, вносят правовую неопределенность в отношении признания авторского права на результаты работы генеративного ИИ на глобальном уровне.

Несколько стран (например, Индия, Ирландия, Новая Зеландия, Южная Африка и Соединенное Королевство) предоставляют авторско-правовую охрану «произведениям, созданным компьютером» без участия авторов-людей. В Украине введены права на «неоригинальные объекты», созданные компьютерными программами.

Рассмотрите возможность применять генеративный ИИ только там, где вопрос прав ИС не имеет существенного значения, например, это может касаться внутреннего использования, генерации идей и кратковременного использования, такого как публикация постов (личных) в социальных сетях.

Контрольный список

Существует множество мер, которые предприятия и организации могут реализовать для обеспечения ответственного и правомерного использования генеративного ИИ. Приведенный ниже контрольный список может быть полезен для предприятий и организаций, стремящихся внедрить ответственную практику и уверенно ориентироваться в этой быстро развивающейся сфере.

Политика для сотрудников и их обучение

- Внедрите политику для сотрудников и проведите обучение, направленные на обеспечение надлежащего использования и поощрение ответственного экспериментирования и применения генеративного ИИ, в том числе:
 - изучите возможности, риски и ограничения, связанные с генеративным ИИ;
 - избегайте использования конфиденциальной информации при формулировании запроса;
 - ограничьте доступ к генеративному ИИ, который был обучен на основе коммерческих тайн, чтобы им могли пользоваться только сотрудники, имеющие доступ к такой информации;
 - избегайте использования сторонних прав ИС в запросах, чтобы свести к минимуму вероятность нарушения прав;
 - избегайте использования инструментов генеративного ИИ, создающих «дипфейки».

Мониторинг рисков и управление профилем риска

- Следите за изменениями в прецедентном праве и нормативных актах.
- Регулярно оценивайте и обновляйте политику с учетом новых рисков и судебных решений.
- Четко доносите информацию о правовых рисках до бизнес-субъектов с целью внедрения практики в соответствии с допустимым для предприятия уровнем риска.
- Ведите список инструментов ИИ, распределяя их по категориям в зависимости от степени риска, например «белые» списки для инструментов, которыми могут пользоваться все сотрудники, инструменты в ограниченном доступе, использующие конфиденциальную информацию, и запрещенные инструменты.

Ведение учета

- Рассмотрите возможность документирования процесса обучения инструментов ИИ.
- Попросите сотрудников маркировать выдаваемые ИИ результаты и вести учет использованных запросов.
- Документально фиксируйте роль человека в процессе создания объектов.

Оценка инструмента ИИ

- Проанализируйте условия и настройки инструментов, предоставляемых внешними поставщиками (включая те, которые были обучены на основе внутренних данных), чтобы
 - знать, сохраняет ли поставщик ваши запросы;
 - знать, на каких данных была обучена модель инструмента;
 - найти инструменты, которые используют обучающие данные, имеющие соответствующую лицензию или являющиеся общественным достоянием, или же содержат технические средства защиты от использования охраняемых данных;
 - определить, предлагает ли поставщик компенсацию за нарушение прав ИС и каковы условия ее выплаты.
- Обеспечьте проверку и мониторинг инструментов генеративного ИИ специалистами по информационной безопасности.
- Изучите частные инструменты генеративного ИИ, которые хранятся на локальных серверах или в частной облачной среде, чтобы повысить уровень контроля и обеспечить гарантии.
 - Добивайтесь от поставщика предоставления соответствующей защиты и гарантий в отношении конфиденциальной информации.



Оценка данных

- Проверяйте наборы данных при обучении ИИ и принимайте во внимание права собственности на ИС и охват лицензий.

Результаты работы ИИ

- Проверяйте условия поставщиков инструментов генеративного ИИ в отношении прав на ИС и права собственности на результаты работы ИИ.
- Проверяйте выдаваемые ИИ результаты на предмет нарушений прав ИС перед их использованием.
- Обеспечьте творческое участие и вклад человека в результаты работы ИИ для сохранения контроля над правом собственности на эти результаты.
- Заключайте договоры о праве собственности на результаты работы ИИ.
- Документально фиксируйте роль человека в процессе создания объектов.
- Получайте необходимое согласие и лицензию на синтез чьего-либо голоса или образа.

