Екатерина Хамидуллина

Партнер, глава практик разрешения споров, права МФЦА и ТМТ

Кирилл Грешников

Старший юрист

Юридическая фирма «AEQUITAS»

АКТУАЛЬНЫЕ ВОПРОСЫ РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КАЗАХСТАНЕ: ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ И ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ БИЗНЕСА

(информация действительна по состоянию на 23 июня 2026 года)

Введение

По мере роста роли искусственного интеллекта государства начали активно формировать нормативную базу, направленную на регулирование данной сферы. Казахстан в данном процессе занимает проактивную позицию и 17 ноября 2025 года в Казахстане был принят Закон Республики Казахстан «Об искусственном интеллекте» (далее – «Закон»), который стал первым специализированным нормативным актом в данной области на пространстве ЕАЭС. Закон вступил в силу 18 января 2026 года.

Принятие Закона меняет правовую среду для бизнеса, использующего или планирующего использовать решения на базе искусственного интеллекта. При этом ключевой интерес для бизнеса представляют не столько формальные нововведения, сколько практические вопросы их применения, включая неопределенности регулирования, потенциальные ограничения, возникающие риски, а также проблемные вопросы применения нового регулирования для бизнеса с целью выявления возможных направлений дальнейшего развития правовой среды.

В рамках настоящей статьи основное внимание будет уделено основным положениям Закона и ряду проблемных аспектов, связанных с ним.

Основные положения Закона

Как и в большинстве законодательных актов, Закон содержит в себя ряд новых терминов, которые являются уникальными для казахстанского законодательства. Среди таких терминов «искусственный интеллект» (далее – «ИИ»), «библиотека данных», «изготовитель библиотеки данных», «пользователь системы ИИ», «уполномоченный орган в сфере искусственного интеллекта» и другие. В Законе содержится15 специальных терминов с определениями.

Закон рассматривает ИИ как функциональную способность к имитации когнитивных функций, характерных для человека, обеспечивающую результаты, сопоставимые с

результатами интеллектуальной деятельности человека или превосходящие их. Несмотря на широкую формулировку, она имеет прикладное значение, поскольку позволяет отделить системы ИИ от иных цифровых решений и тем самым определить сферу применения регуляторных требований.

При этом в Законе имеются существенные пробелы, связанных с тем, что законодательно не предусмотрены такие важные понятия, как разработчик системы ИИ, дистрибьютор системы ИИ и интегратор системы ИИ. Из-за отсутствия регуляций и определений данных лиц сложно разграничить ответственность лиц, работающих с ИИ, и, как следствие, установить виновных, ответственных и т.д. Отсутствие четкого разграничения статусов между транснациональными поставщиками (например, OpenAI), локальными IT-компаниями, выступающими интеграторами системы ИИ, и казахстанскими владельцами ИИ создает серьезные сложности при определении зон ответственности и установлении виновных лиц в случае причинения ущерба.

Ключевой особенностью Закона является внедрение риск-ориентированного подхода. Системы ИИ классифицируются по трем уровням риска в зависимости от их потенциального воздействия на права, безопасность и интересы людей, при этом бремя первичной квалификации возлагается на собственника, владельца системы ИИ или оператора национальной платформы ИИ. К системам минимальной степени риска относятся те системы ИИ, нарушение или прекращение функционирования которых окажет минимальное влияние на их пользователей. Системы ИИ средней степени риска охватывают системы, нарушение или прекращение функционирования, которых может привести к снижению эффективности и результативности деятельности пользователей, а также причинить им моральный вред или нанести материальный ущерб. Системы ИИ высокой степени риска способны спровоцировать чрезвычайные ситуации социального или техногенного характера и/или повлечь значительные негативные последствия для обороны, экономики, безопасности, международных отношений, отдельных сфер хозяйства, пользователей, инфраструктуры Казахстана, жизнедеятельности физических лиц.

Для систем ИИ высокого риска Закон устанавливает более строгий режим регулирования. Например, в отношении систем ИИ высокого риска, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры предусматривается обязательное проведение аудита с привлечением специализированных аудиторов, ведение расширенной технической документации, включая описание архитектуры, алгоритмов и используемых данных, а также внедрение непрерывного процесса управления рисками на протяжении всего жизненного цикла системы. Подобные системы обязаны пройти испытания на соответствие требованиям информационной безопасности в соответствии с законодательством.

Для бизнеса это означает необходимость выстраивания внутренних комплаенс-процедур самого высокого уровня. Кроме того, Закон классифицирует системы ИИ по степени автономности: от низкой, где алгоритм лишь подготавливает варианты решений для человека, до высокой, где корректировка принятых машиной решений человеком полностью исключена либо технически невозможна.

Отдельный блок Закона посвящен прозрачности использования ИИ технологий.

Законом установлено, что распространение синтетических результатов деятельности систем ИИ допускается только при условии их маркировки в машиночитаемой форме и сопровождения визуальной либо иной формы предупреждения, обеспечивающей возможность восприятия пользователем без применения методов, затрудняющих такое восприятие.

Компании, использующие чат-боты и генеративные модели для взаимодействия с клиентами/пользователями, теперь обязаны прямо уведомлять их о порядке и

последствиях автоматизированной обработки данных, о возможности заявить возражение против автоматизированной обработки, а также о порядке защиты своих прав, свобод и законных интересов.

На собственников и владельцев систем ИИ также возложены следующие обязанности:

1) осуществление управления рисками систем ИИ;

2) принятие мер для обеспечения безопасности и надежности систем ИИ, включая защиту от несанкционированного доступа, сбоев в их работе;

3) ведение документации на систему ИИ в зависимости от степени ее воздействия на безопасность, права, свободы и законные интересы физических лиц, общественный порядок в соответствии с перечнем документации на системы ИИ;

4) осуществление технической поддержки пользователей по вопросам функционирования систем ИИ;

5) предоставление пользователям возможности ознакомиться с пользовательским соглашением системы ИИ до начала её использования.

В первую очередь, Закон обязывает выстроить непрерывный процесс управления рисками, который должен осуществляться на протяжении всего жизненного цикла алгоритма и включать:

1) выявление и анализ известных и прогнозируемых рисков системы ИИ при использовании в соответствии с ее предполагаемым назначением;

2) оценку рисков системы ИИ, осуществляемую в соответствии с ее предполагаемым назначением и в условиях предсказуемого нецелевого использования;

3) принятие соответствующих и целенаправленных мер по управлению рисками, предназначенных для предупреждения и устранения выявленных рисков;

4) регулярное, не реже одного раза в год, обновление рисков.

Отдельное внимание уделяется превентивным мерам по обеспечению безопасности и надежности систем ИИ. Эксплуатация таких алгоритмов должна вестись в защищенной среде, исключающей несанкционированный доступ, критические программные сбои и возможность злоупотреблений.

Определенная административная нагрузка на разработчиков систем ИИ связана с правилами ведения технической документации. Полагаем, что в данном случае должен применяться риск-ориентированный подход, при котором объем и глубина раскрываемой информации напрямую зависят от степени потенциального воздействия системы ИИ на общественный порядок, а также фундаментальные права и свободы граждан. Следовательно, для высокорисковых решений клиентам потребуется формировать развернутые технические файлы и лог-журналы.

В целях защиты прав конечных потребителей также закрепляется обязанность по осуществлению постоянной технической поддержки. Это требует от компаний-владельцев выделения ресурсов на создание службы поддержки, функционал которой позволит пользователям своевременно получать разъяснения по логике работы алгоритма, а также оперативно сообщать о системных ошибках или некорректной выдаче данных.

Также важной обязанностью является необходимость предоставления пользователю возможности ознакомиться с пользовательским соглашением до фактического начала использования системы ИИ. Как правило в таком документе закрепляются ограничения ответственности разработчика системы ИИ, правила обработки вводимых запросов, рамки применимости технологии и иные вопросы. При всем этом законодатель разумно не требует раскрытия исходного кода, позволяя сохранить коммерческую тайну.

Одновременно вводится строгий перечень, запрещающий создание и эксплуатацию систем ИИ, обладающих одной из следующих функциональных возможностей:

1) использование подсознательных, манипулятивных или иных методов, искажающих поведение физического лица и ограничивающих способность принимать осознанные решения или вынуждающих принимать решения, которые могут причинить вред или создать угрозу причинения вреда;

2) использование моральной и (или) физической уязвимости физического лица из-за возраста, инвалидности, социального положения и любых иных обстоятельств с целью причинения или создания угрозы причинения вреда лицу;

3) оценку и классификацию физических лиц или группы лиц в течение определенного периода времени на основе их социального поведения или известных, предполагаемых или прогнозируемых личных характеристик, за исключением случаев, предусмотренных законодательством;

4) сбор и обработку персональных данных с нарушением казахстанского законодательства;

5) классификацию физических лиц на основе их биометрических данных для формирования выводов об их расе, политических взглядах, религиозной принадлежности, и по любым иным обстоятельствам (критериям) в целях использования для какой-либо дискриминации физического лица;

6) определение эмоций физического лица без его согласия, за исключением случаев, предусмотренных законодательством;

7) создание и распространение запрещенных законами РК результатов деятельности систем ИИ.

По своей сути данные ограничения во многом схожи с подходами, закрепленными в европейском регулировании, и отражают общий международный тренд на ограничение наиболее чувствительных сценариев использования ИИ.

Вступление в силу новых регуляций повлекло системные изменения и в смежных отраслях права. Так, теперь в отношении защиты потребителей появилось новое требование, применимое к продавцам (изготовителям, исполнителям) работающими с товарами (услугами), содержащими компоненты ИИ. С принятием Закона на таких лиц возложена обязанность по информированию потребителя о возможном риске и об условиях безопасного использования товара (работы, услуги), содержащего/й компоненты ИИ (произведенного, выполняемой и (или) оказываемой системой ИИ), путем указания необходимой информации в документации, прилагаемой к товару (работе, услуге), на потребительской таре, этикетках или иным способом, принятым для отдельных видов товаров (работ, услуг).

В области защиты персональных данных установлен запрет на автоматизированную обработку, изменяющую законные права субъекта, без его явного согласия. С введением Закона запрещаются сбор, обработка персональных данных для создания или расширения баз данных посредством нецелевого извлечения персональных данных из общедоступных источников.

Особый интерес для практики представляет создание института доверенных систем ИИ высокой степени риска, перечни которых формируются государственными органами для внедрения лучших отраслевых практик. Включение в такой реестр требует прохождения обязательного аудита, в рамках которого проверяется не только информационная безопасность, но и качество, а также правомерность использования библиотек данных для обучения.

Риски и возможности для бизнеса

Введение специального регулирования в сфере ИИ непосредственное оказывает прямое влияние на деятельность казахстанских компаний, использующих ИИ в операционных, маркетинговых, управленческих или иных бизнес-процессах. Закон формирует для бизнеса новую правовую и комплаенс-среду, в которой использование ИИ требует не только технологической, но и юридической и регуляторной зрелости. Компании, способные встроить требования регулирования в свои бизнес-процессы, смогут не только минимизировать риски, но и извлечь дополнительные преимущества из растущего рынка ИИ. При этом Закон формирует не только дополнительные ограничения и обязанности, но и создает определенные возможности, связанные с повышением прозрачности рынка и доверием со стороны потребителей и контрагентов.

Ключевым риском, который можно выделить в связи с Законом, является новая регуляторная нагрузка, возлагаемая на бизнес. Компании, применяющие решения на базе ИИ, фактически становятся субъектами специального регулирования и обязаны выстраивать внутренние процессы с учетом требований Закона. В данном случае речь идет, в первую очередь, о необходимости классификации используемых ИИ систем по уровням риска, ведении технической документации, внедрении процедур управления рисками, а в отдельных случаях прохождение аудита. Для многих компаний (особенно для малого бизнеса) это означает необходимость создания новых или адаптации существующих внутренних комплаенс-процедур, что влечет дополнительные организационные и финансовые издержки.

При этом размер административных штрафов не является высоким для среднего и крупного бизнеса. Однако не исключено, что правоприменительная практика в данной сфере, с высокой вероятностью, может сопровождаться повышенным вниманием со стороны регуляторов, общества и СМИ, что дополнительно повышает затраты для бизнеса. Для компаний, работающих в публичном поле, включая банки, телеком-операторов и цифровые платформы, подобные риски могут иметь более существенные последствия, чем сам штраф и связаны с репутационными рисками.

Использование ИИ напрямую связано с рисками в отношении обработки данных. Зачастую использование ИИ предполагает активную работу с персональными данными пользователей. Ранее такие данные уже подлежали защите в соответствии с законодательством о защите персональных данных и информатизации. С введением в действие Закона был установлен дополнительный режим защиты таких данных, усилены требования к защите данных пользователей и ограничена возможность передачи таких данных третьим лицам, включая иностранные платформы, без надлежащего согласия пользователя. Для бизнеса это означает необходимость пересмотра практики использования облачных решений, а также проведение более тщательной юридической оценки условий работы с поставщиками ИИ сервисов. Нельзя не отметить, что в отличие от судебной практики по ИИ, судебная практика по ответственности за нарушения в сфере персональных данных сформирована в достаточной степени и указывает на то, что компании часто привлекаются к ответственности за нарушения в данной сфере.

Следующим существенным риском для бизнеса является закрепление в Законе принципа прямой ответственности за деятельность систем ИИ. Закон устанавливает, что все субъекты, участвующие в создании, внедрении и эксплуатации ИИ, несут ответственность за функционирование соответствующих систем ИИ и за результаты их работы с учетом своей роли на каждом этапе жизненного цикла.

Фактически законодатель исходит из расширительного подхода к определению круга потенциально ответственных лиц. В зоне риска оказываются не только разработчики и владельцы систем ИИ, но и иные лица, взаимодействующие с ИИ (даже если регуляции в отношении таковых отсутствуют, как, например, интеграторы, дистрибьютеры, поставщики

и т.п.), а в отдельных случаях даже конечные пользователи, если их действия повлекли нарушение требований законодательства. Для бизнеса это означает, что использование ИИ перестает быть исключительно технологическим инструментом и становится источником самостоятельного юридического риска, требующего отдельного управления.

Прямо установлено, что ответственность за создание и эксплуатацию системы ИИ несут все субъекты, осуществляющие данные действия. Закон закрепляет разграничение ролей между собственником, владельцем системы ИИ и пользователем системы ИИ. Эти лица обязаны обеспечивать постоянный контроль над системой ИИ в объеме и порядке, зависящих от их роли, на всех этапах жизненного цикла системы ИИ.

При этом на практике нельзя исключать перераспределение ответственности между участниками всей цепочки, например, в случае, если вред возник вследствие особенностей самой модели ИИ, недостатков обучения или отсутствия встроенных ограничений, претензии могут быть предъявлены не только к пользователю, но и к разработчику или владельцу системы ИИ. Всё это влечет за собой не только необходимость распределения технических вопросов между всеми участниками пользования ИИ, но и необходимость более тщательной проработки отношений между всеми участниками, включая распределение ответственности.

Исходя из текущих положений Закона, разумно предположить, что собственник или владелец системы ИИ могут нести ответственность по принципу своего виновного поведения или халатности. Вина владельца системы ИИ заключается в неверном выборе технологии для специфического контекста (например, использование потребительского чат-бота для скоринга кредитоспособности), неспособности провести аудит предвзятости применительно к своей клиентской базе, неправомерном сборе данных для обучения модели, отказе от внедрения процессов обязательного человеческого контроля и т.п.

Ответственность пользователя, вероятно, традиционно, будет ограничиваться рамками его умышленных противоправных действий. Пользователь может нести ответственность за характер вводимых запросов и за осознанные незаконные решения, принятые им на основе рекомендаций ИИ. При этом полагаем, что в силу того, что обычные пользователи далеко не всегда понимают грань между запрещенным и дозволенным, ответственность пользователя разумно было бы ограничить в тех случаях, когда разработчик системы ИИ не обеспечил внедрение базовых механизмов контроля и ограничений для собственной системы ИИ (например, направленных, в частности, на предотвращение генерации ответов на недопустимые либо потенциально противоправные запросы пользователей).

Важно отметить, что понятие и роль «разработчика системы ИИ» не предусмотрены в Законе, что усложняет определение уровня его ответственности в этой сфере. Закон оперирует лишь такими субъектами, как собственник, владелец системы ИИ и пользователь. При этом разработчики системы ИИ не всегда являются собственниками, владельцами системы ИИ и пользователями ИИ. Учитывая то, что ответственность субъекта зависит от его роли на соответствующем этапе жизненного цикла системы ИИ, то соответственно, отсутствие регуляций деятельности разработчика системы ИИ не означает что у них нет никаких обязательств и ответственности. В данном случае разработчик системы ИИ будет нести ответственность на общих основаниях исходя из своей роли.

Можно предположить, что разработчик системы ИИ отвечает за техническую корректность, безопасность и соблюдение установленных ограничений на этапе создания системы ИИ. Мы полагаем, что на разработчике системы ИИ должна лежать объективная ответственность за архитектурные дефекты системы ИИ, включающие в себя ответственность за безопасность ответов, отсутствие встроенных механизмов безопасности и этических ограничителей, а также за изначальную, алгоритмически заложенную предвзятость модели. Вероятен риск, что если ИИ позволяет пользователю незаконно практиковать какой-либо вид деятельности (юриспруденция, экономика,

медицина и т.п.) и подобная практика повлекла ущерб для третьих лиц, то потенциальная ответственность косвенно может быть возложена не только на пользователя, но и на разработчика систем ИИ.

Институт гражданско-правовой ответственности в сфере ИИ осложнён тем, что в Гражданском кодексе РК в настоящее время отсутствуют специализированные нормы, регулирующие порядок возмещения вреда, причиненного автономными действиями систем ИИ. В этой связи при разрешении вопросов ответственности вероятно придется по аналогии применять общие нормы о деликтах (обязательствах, возникающих вследствие причинения вреда). Однако классический деликт традиционно требует обязательного доказывания противоправного деяния, вины причинителя и прямой причинно-следственной связи. Доказать вину конкретного программиста или владельца системы ИИ, когда вред причинен в результате многослойного машинного обучения, в рамках текущего законодательства практически невозможно.

Отдельное значение приобретает риск, связанный с принятием решений на основе алгоритмов. Если ранее принятие дискриминационных решений было запрещено исходя из общего подхода и принципов законодательства, что усложняло процесс доказывания и привлечения нарушивших лиц к ответственности, то теперь Закон прямо запрещает любые дискриминационные практики при использовании ИИ с нарушением прав и законных интересов лиц. На практике это означает, что компании должны обеспечивать корректность и обоснованность решений, принимаемых с использованием ИИ, особенно в чувствительных сферах.

Дополнительный риск также связан с возможностью предъявления требований о возмещении вреда. Закон прямо закрепляет, что возмещение вреда, причиненного системами ИИ, осуществляется в общем порядке, что может говорить о том, что собственники систем ИИ несут ответственность за причиненный вред (включая имущественный, репутационный и в отдельных случаях моральный).

Вопросы ответственности за работу с ИИ в целом можно выделить в отдельную и самостоятельную публикацию. Ввиду обширности возможных нарушений при работе с ИИ, данный вопрос требует отдельного внимания. Ниже перечислены основные тезисы, относящиеся к вопросам ответственности.

С точки зрения технической и правовой природы ИИ, можно выделить три ключевых блока ответственности, которые могут возникнуть при использовании ИИ:

1) Административная ответственность, которая прямо предусмотрена законодательством Казахстана (в рамках КоАП).

2) Гражданско-правовая ответственность, которая возникает в случае причинения вреда и ущерба в результате использования систем ИИ. Закон прямо отсылает к применению общих положений гражданского законодательства, в частности норм о возмещении вреда и ущерба.

3) Договорная ответственность, которая приобретает ключевое значение в отношениях между участниками цепочки создания и использования ИИ. В рамках договоров между разработчиками, поставщиками, интеграторами и конечными пользователями стороны вправе детально распределять риски, включая установление ограничений ответственности, гарантий, условий использования данных и порядка реагирования на инциденты.

Как было отмечено выше, особенностью текущего регулирования является то, что Закон закрепляет принцип распределенной ответственности, в рамках которого потенциально ответственными могут являться несколько субъектов одновременно в зависимости от их роли.

Например, если вред возник вследствие некорректного обучения модели ИИ или отсутствия необходимых ограничений, претензии могут быть предъявлены разработчику системы ИИ. Если система ИИ использовалась с нарушением инструкций или без учета требований законодательства, ответственность, с высокой вероятностью, будет возложена на владельца или пользователя системы ИИ.

В качестве примера можно рассмотреть типовую ситуацию в финансовом секторе, в которой кредитные организации зачастую используют систему ИИ для оценки кредитоспособности клиента. В случае если система ИИ принимает решение об отказе на основании некорректных или дискриминационных данных, клиент вправе оспорить такое решение. В рамках спора могут возникнуть вопросы о том, была ли модель ИИ обучена надлежащим образом, имела ли кредитная организации возможность проверить корректность ее работы и обеспечила ли она необходимый уровень контроля. В зависимости от этих обстоятельств ответственность может быть распределена между кредитной организацией как владельцем и поставщиком системы ИИ, как разработчиком системы ИИ.

Отдельно следует отметить риски, связанные с непрозрачностью внутренних процессов работы ИИ. Для многих моделей ИИ характерна ограниченная объяснимость принимаемых решений, что уже само по себе создает сложности с точки зрения доказательства правомерности их функционирования. В условиях действия Закона отсутствие надлежащей документации, журналов работы и процедур внутреннего контроля может существенно осложнить защиту позиции компании при проверках со стороны регуляторов или при рассмотрении возможных споров.

Без выстроенной системы управления рисками и внутреннего контроля компания фактически лишается возможности подтвердить, что она предпринимала разумные меры для предотвращения нарушений. Это особенно критично для систем ИИ, отнесенных к категории высокого риска, где требования к прозрачности и контролю являются повышенными. Соответственно, для бизнеса становится принципиально важным не только внедрение ИИ решений, но и обеспечение их документируемости, прослеживаемости и управляемости не только с технической, но и юридической, и управленческой точек зрения.

Следует отметить, что значительная часть перечисленных выше рисков не является принципиально новой для бизнеса. Компании, активно внедряющие цифровые решения, ранее уже сталкивались с вопросами ответственности за автоматизированные процессы, обеспечения защиты персональных данных, прозрачности алгоритмов и недискриминационности принимаемых решений. Принятие Закона в данном случае не столько создает новые категории рисков, сколько формализует и усиливает уже существующие требования, переводя их в сферу прямого правового регулирования и контроля.

Важно отметить и то, что формализация правил использования ИИ повышает предсказуемость правовой среды. Для инвесторов и технологических партнеров наличие понятного регулирования зачастую является ключевым фактором при принятии решений о выходе на рынок или масштабировании проектов. В этом смысле Закон выполняет не только ограничительную, но и стимулирующую функцию, создавая основу для развития экосистемы ИИ в Казахстане.

Практические рекомендации для бизнеса

В заключении можно выделить ряд рекомендаций, которые представляются обоснованными с точки зрения минимизации рисков бизнеса и обеспечения соответствия требованиям Закона:

1) Компаниям рекомендуется утвердить внутреннюю ИИ-комплаенс политику для распределения зон ответственности, а также сформировать единый реестр используемых

ИИ алгоритмов и программного обеспечения. Данные меры позволят установить прозрачные правила контроля над ИИ инфраструктурой и обеспечить защиту объектов информатизации.

2) Рекомендуется провести аудит правомерности происхождения информации, используемой для текущего машинного обучения (что информация, используемая для обучения модели, получена законным образом и не нарушает авторских, коммерческих или персональных прав), и документировать процессы обеспечения информационной безопасности таких процессов. Необходимо осуществлять сбор и дальнейшую обработку персональных данных пользователей при наличии предварительного согласия пользователя на такой сбор и обработку.

3) В целях формирования доказательственной базы следует разработать внутренние технические паспорта с описанием архитектуры каждой ИИ-системы. Дополнительно рекомендуется внедрить маркировку сгенерированного контента, чтобы исключить риск введения пользователей в заблуждение.

4) Важно пересмотреть действующие контракты, соглашения о конфиденциальности и пользовательские соглашения, в которых следует прямо закрепить условия использования ИИ и разграничить пределы ответственности за возможные системные ошибки или сбои системы ИИ.

5) Для защиты от финансовых потерь рекомендуется применять механизмы добровольного страхования ответственности и имущественных интересов. Параллельно рекомендуется организовать регулярный аудит ИИ алгоритмов и сбор обратной связи пользователей для выявления технических уязвимостей.

***

Пр. Абая 47, офис 2, г. Алматы
050000 Республика Казахстан
+7 727 3 968 968
aequitas@aequitas.kz