

Риски использования МСР-сервера и ИИ-агентов

Настоящий документ описывает возможные риски, связанные с подключением брокерского счёта к системам искусственного интеллекта с использованием МСР-сервера ООО «Компания БКС» (далее — Компания), и содержит рекомендации по их снижению. Документ подлежит прочтению до выпуска Токена API и начала использования МСР-сервера.

1. Общие положения и разграничение ответственности

1.1. МСР (Model Context Protocol) — открытый протокол подключения внешних сервисов к системам искусственного интеллекта. МСР-сервер Компании — реализация этого протокола, которая позволяет Клиенту подключить свой брокерский счёт к используемому им ИИ-агенту (далее — ИИ-агент), получать данные счёта и рынка, а также направлять торговые поручения через Торговый API Компании.

1.2. ИИ-агент не является программным обеспечением Компании. Компания не разрабатывает, не предоставляет, не настраивает и не контролирует ИИ-агентов, используемых Клиентом (включая, но не ограничиваясь: ChatGPT, Claude, Gemini, Cursor, иные решения, поддерживающие МСР), а также не контролирует их обновления, внутреннюю логику, качество ответов и порядок взаимодействия с Клиентом.

1.3. Выбор ИИ-агента, условия его использования, порядок хранения и обработки передаваемых в него данных определяются Клиентом самостоятельно и регулируются соглашением между Клиентом и поставщиком соответствующего ИИ-сервиса. Компания не является стороной такого соглашения.

1.4. Компания исполняет поручения, поступившие с использованием действующего Токена API Клиента, в порядке, предусмотренном Регламентом оказания услуг на рынке ценных бумаг (далее — Регламент). Поручение, направленное через ИИ-агента с использованием Токена API Клиента, считается направленным Клиентом.

1.5. Компания не предоставляет инвестиционных рекомендаций через МСР-сервер и ИИ-агентов. Ответы, расчёты, выводы и предложения, формируемые ИИ-агентом, не являются индивидуальной инвестиционной рекомендацией Компании и не согласованы с ней.

1.6. Использование МСР-сервера и ИИ-агента не изменяет порядок и условия использования Торгового API, установленные Регламентом. Клиент обязан соблюдать указанные условия в полном объёме независимо от того, направляются запросы и поручения непосредственно Клиентом или через ИИ-агента, включая требования к перечню инструментов, видам сделок, типам, количеству и объёму заявок, частоте направления запросов, а также обязанность самостоятельно знакомиться с вносимыми изменениями. Актуальная редакция Регламента размещена по адресу: bcs.ru/regulatory/additional-archive.

2. Возможные риски, связанные с работой ИИ-агента

2.1. В настоящем разделе описаны возможные риски. Приведённый перечень не является исчерпывающим: при использовании систем искусственного интеллекта могут возникать и иные риски, в том числе ранее не известные. Любые ответы, расчёты и выводы ИИ-агента подлежат самостоятельной проверке (валидации) Клиентом до принятия решений и совершения операций.

2.2. Риск некорректной интерпретации запроса. ИИ-агент может понять запрос Клиента иначе, чем Клиент предполагал, в том числе определить иной инструмент, иное количество, иную цену, иной тип или направление поручения.

2.3. Риск недостоверного ответа (галлюцинации). Системам искусственного интеллекта свойственно явление, при котором модель формирует правдоподобный по форме, но не соответствующий действительности ответ (галлюцинация). ИИ-агент может указать несуществующие данные, инструменты или события, привести ошибочные расчёты, сослаться на несуществующие источники, а также представить предположение как установленный факт. Такое поведение является особенностью технологии и может возникать в том числе при корректной передаче данных через Торговый API.

2.4. Риск ошибочной интерпретации рыночных данных. ИИ-агент может неверно сопоставить данные, использовать устаревшие или неполные сведения, неверно учесть параметры инструмента, лоты, валюту расчётов, режим торгов, корпоративные события.

2.5. Риск непредсказуемого изменения поведения. Поставщик ИИ-сервиса вправе в любой момент изменить модель, её версию, настройки и ограничения без уведомления Клиента и Компании. Поведение ИИ-агента, корректное ранее, может измениться.

2.6. Риск автономных действий. Клиент может настроить ИИ-агента таким образом, что он будет формировать и направлять поручения без дополнительного подтверждения со стороны Клиента по каждому поручению. Такая конфигурация определяется Клиентом и существенно повышает риск убытков.

2.7. Риск отсутствия подтверждения на стороне Компании. Порядок подтверждения действий Клиентом реализуется в интерфейсе ИИ-агента и находится вне контроля Компании. Компания не может гарантировать наличие, корректность и неизменность такого подтверждения.

3. Возможные риски, связанные с направлением и исполнением поручений

3.1. В настоящем разделе описаны возможные риски. Приведённый перечень не является исчерпывающим.

3.2. Риск расхождения сведений о статусе поручения. ИИ-агент может сообщить Клиенту о неуспешном направлении поручения в то время, как поручение было принято

и исполнено Компанией, и наоборот. Причинами могут быть сетевые сбои, превышение времени ожидания ответа, некорректная обработка ответа Торгового API на стороне ИИ-агента.

3.3. Риск повторного направления поручения. При получении ошибки или отсутствии ответа ИИ-агент может повторно направить поручение, что может привести к направлению нескольких поручений и совершению сделок в большем объёме, чем предполагал Клиент. В Торговом API предусмотрен механизм идемпотентности: повторное направление поручения с тем же идентификатором не приводит к созданию нового поручения. При этом Компания не контролирует и не может гарантировать, что ИИ-агент при повторном обращении использует прежний идентификатор, а не сформирует новый и не направит тем самым новое поручение.

3.4. Риск задержки. Передача данных через ИИ-агента может сопровождаться задержками, в том числе существенными. Рыночные условия к моменту исполнения поручения могут отличаться от условий на момент формирования запроса.

3.5. Источник данных и причина возможных расхождений. Торговый API Компании предоставляет достоверные сведения о составе портфеля, статусе поручений, совершённых сделках, остатках и обязательствах Клиента. Расхождения между тем, что Клиент видит в диалоге с ИИ-агентом, и фактическим состоянием счёта могут возникать не из-за данных Компании, а на стороне ИИ-агента: при обработке ответа Торгового API, его интерпретации, сокращении, пересказе или использовании ранее полученных и уже неактуальных сведений.

3.6. Приоритет официальных интерфейсов. Юридически значимыми и подлежащими применению во взаимоотношениях Сторон являются сведения, отражённые в личном кабинете, мобильном приложении, торговом терминале и отчётах Компании. Представление данных в интерфейсе ИИ-агента носит справочный характер.

3.7. Рекомендация. Клиенту следует самостоятельно проверять (валидировать) ответы ИИ-агента, в том числе сведения о составе портфеля, рыночных данных, статусе поручений и совершённых сделках, сверяя их с данными официальных интерфейсов Компании, и не полагаться на представление информации в интерфейсе ИИ-агента как на единственный источник.

4. Возможные риски несанкционированного доступа

4.1. Токен API является аналогом собственноручной подписи Клиента. Любые действия, совершённые с его использованием, считаются совершёнными Клиентом.

4.2. Передача Токена API третьим лицам, его сохранение в переписке, в облачных сервисах, в репозиториях кода, в журналах и в истории чатов может создать риск несанкционированного доступа к счёту.

4.3. ИИ-агент и связанные с ним сервисы могут сохранять историю диалога, включая переданные в них данные. Клиенту следует исходить из того, что любая информация, направленная в ИИ-агента, может быть сохранена поставщиком соответствующего сервиса.

4.4. Клиенту следует незамедлительно отозвать Токен API в личном кабинете при подозрении на его компрометацию, при смене устройства, при прекращении использования ИИ-агента, а также при передаче устройства третьим лицам.

5. Возможные риски, связанные с передачей данных третьим лицам

5.1. При использовании ИИ-агента данные о счёте Клиента, составе портфеля, совершённых сделках, остатках и операциях передаются поставщику ИИ-сервиса, выбранному Клиентом, и обрабатываются на его инфраструктуре.

5.2. Поставщик ИИ-сервиса может находиться за пределами Российской Федерации. В этом случае данные Клиента передаются трансгранично, и на такую передачу могут не распространяться гарантии, предусмотренные законодательством Российской Федерации в отношении обработки данных на её территории.

5.3. Поставщик ИИ-сервиса может использовать переданные данные для обучения и улучшения своих моделей, если иное не предусмотрено его условиями или не отключено Клиентом в настройках.

5.4. Компания не контролирует и не несёт ответственности за сохранность, конфиденциальность, срок хранения и дальнейшее использование данных, переданных Клиентом в ИИ-агента.

5.5. Клиент самостоятельно оценивает допустимость передачи указанных сведений третьим лицам, в том числе с учётом требований законодательства о персональных данных, о коммерческой тайне и внутренних правил организации, если Клиент является её работником или представителем.

6. Возможные риски, связанные с использованием биржевой информации

6.1. Рыночные данные (котировки, сведения о заявках и сделках, иная биржевая информация) предоставляются организатором торговли на условиях, ограничивающих их дальнейшее распространение, передачу третьим лицам и использование в коммерческих целях.

6.2. При передаче биржевой информации в ИИ-агента такая информация поступает в распоряжение третьего лица — поставщика ИИ-сервиса, который может сохранять, обрабатывать и использовать её способами, не контролируемые ни Клиентом, ни Компанией.

6.3. Клиент самостоятельно несёт ответственность за соблюдение условий использования биржевой информации, включая ограничения на её распространение и перераспределение, а также за последствия передачи такой информации третьим лицам.

6.4. Использование биржевой информации для создания производных информационных продуктов, их публикации или предоставления третьим лицам может требовать отдельного соглашения с организатором торговли.

7. Возможные технические риски

7.1. Возможны временная недоступность МСР-сервера, Торгового API, сервисов организатора торговли, каналов связи и сервисов поставщика ИИ.

7.2. Возможны ограничения по числу запросов в единицу времени, при превышении которых часть запросов ИИ-агента не будет обработана.

7.3. Возможны изменения в составе и формате данных, предоставляемых через Торговый API, которые потребуют адаптации на стороне ИИ-агента или используемых Клиентом программных средств.

7.4. Компания вправе ограничить или приостановить доступ к МСР-серверу и Торговому API в случаях, предусмотренных Регламентом, в том числе при выявлении аномальной активности, угрозы безопасности или нарушения условий использования.

8. Рекомендации по снижению рисков

8.1. Начинать использование с Токена API, предоставляющего доступ только на чтение данных, и переходить к токену с правом направления поручений только после того, как Клиент убедился в корректности работы выбранного ИИ-агента.

8.2. Не настраивать автоматическое направление поручений без подтверждения Клиентом каждого поручения.

8.3. Проверять результат каждой операции в личном кабинете или мобильном приложении Компании.

8.4. Использовать отдельный Токен API для каждого ИИ-агента и отзывать неиспользуемые токены.

8.5. Не передавать Токен API третьим лицам и не вводить его в переписку, в том числе в диалог с ИИ-агентом.

8.6. Использование локально развёрнутых моделей. Клиент вправе использовать языковые модели, развёрнутые на собственном оборудовании или в контролируемом им контуре. При таком использовании данные счёта и биржевая информация не передаются внешним поставщикам ИИ-сервисов, что существенно снижает риски, описанные в разделах 5 и 6 настоящего документа. Компания не предоставляет такие модели, не оказывает услуг по их развёртыванию и не несёт ответственности за их работу. При

недостаточности собственных компетенций Клиенту рекомендуется привлечь профильных специалистов для получения экспертной помощи и консультации по настройке безопасного контура использования ИИ-агента.

8.7. Ознакомиться с условиями обработки данных выбранного ИИ-сервиса и при наличии технической возможности отключить использование передаваемых данных для обучения моделей.

8.8. Не использовать ИИ-агента в качестве единственного источника сведений при принятии инвестиционных решений и самостоятельно проверять (валидировать) получаемые от него ответы.

8.9. Соблюдать условия использования Торгового API, установленные Регламентом, в том числе при направлении запросов и поручений через ИИ-агента, и самостоятельно знакомиться с вносимыми в Регламент изменениями.

9. Ответственность

9.1. Компания не предоставляет Клиенту каких-либо гарантий по обеспечению постоянного, бессрочного и бесперебойного обмена сообщениями посредством Торгового API и не гарантирует получение Компанией сообщения (запроса, информации, поручения) от Рабочего места Клиента (API). Компания не несёт ответственности за возможные убытки Клиента в результате непринятия к исполнению и (или) неисполнения поручения на совершение торговой операции либо поручения на отмену поручения на совершение торговой операции в случае несоответствия его требованиям Регламента.

9.2. Компания не несёт ответственности за убытки Клиента, возникшие вследствие некорректной работы ИИ-агента, ошибочной интерпретации им запросов и данных, автономных действий ИИ-агента, настроек, установленных Клиентом, а также вследствие передачи данных третьим лицам при использовании ИИ-агента.

9.3. Использование MCP-сервера и ИИ-агента означает, что Клиент ознакомился с настоящим документом, понимает описанные в нём риски, осознаёт их возможные последствия и принимает такие риски на себя в полном объёме, включая риск возникновения убытков.