Финансовый брокер и ИИ: что работает, а что — миф

Анастасия НАЙШЕВА,
руководитель отдела ИИ-автоматизации, «АВИ Кэпитал»

Неразумно отрицать очевидный технологический прогресс, который перестал быть модным дополнением и даже уже не стадией тестирования гипотез, а становится гармоничным инструментом в руках профессионалов с большой долей опыта и трезвого здравомыслия. Мессия пришел, но оказался стажером с энциклопедическими знаниями и избирательной памятью. Разберем основные неопределенности и мифы про ИИ.

Искусственный интеллект работает ровно настолько хорошо, насколько качественны данные, которыми его кормят

МИФ ПЕРВЫЙ: «ЭТО ЖЕ ИИ, ОН ВСЁ ЗНАЕТ»

Начнем с самого живучего заблуждения. Большая языковая модель производит впечатление всезнающего оракула ровно до того момента, пока вы не начнете проверять ее ответы. Именно тогда выясняется, что система способна с академической уверенностью процитировать несуществующий нормативный акт Банка России, сослаться на судебную практику, которой не было, и выдать финансовый показатель, взятый буквально из воздуха. Всё это — идеально звучащие галлюцинации (тут многие бы позавидовали умению так красиво лгать).

Помимо этого, необходимо помнить, что если модель развернута локально (а это единственный вариант для корректной безопасной работы с данными, что критично для любой брокерской компании), то у нее есть ограничения по глубине данных, на которых она обучалась, и именно поэтому она не ответит на вопрос «какая сейчас ставка Банка России» без вспомогательных источников.

Для брокерской деятельности галлюцинации не абстрактная проблема. Когда речь идет о расчете маржинальных требований, интерпретации условий договора или анализе рисков портфеля, ценой ошибки является не просто репутация, а деньги клиента и ответственность перед регулятором. Поэтому первое, что мы внедрили вместе с искусственным интеллектом, — обязательная верификация каждого вывода. Парадокс: чтобы автоматизировать проверку, нам понадобились люди, которые проверяют автоматизацию.

МИФ ВТОРОЙ: «ОН ЗАМЕНИТ СОТРУДНИКОВ»

Реальность оказалась куда прозаичнее: искусственный интеллект не заменяет людей — он меняет характер их работы.

Аналитик, который раньше вручную собирал данные из пяти систем и формировал отчет за три часа, теперь получает черновик за семь минут. Но черновик нужно проверить, скорректировать, дополнить контекстом, который система попросту не имела. Естественно, это работа сообща:

мы собираем агентов с ядром в виде языковой модели и даем ему необходимые источники данных, то есть инструменты. В итоге аналитик работает больше, быстрее и с более высокими требованиями к качеству результата. Процесс итеративный и требует вовлеченности знатоков. **Штат мы не сокращаем — мы перераспределяем усилия.**

ТЕХНИЧЕСКИЕ СЛОЖНОСТИ, О КОТОРЫХ НЕ ПИШУТ В ПРЕЗЕНТАЦИЯХ

Любой вендор, продающий решение на основе искусственного интеллекта, покажет вам красивый слайд с архитектурой и пообещает интеграцию «за несколько недель». После подписания договора выяснится, что ваша учетная система хранит данные в формате, разработанном в эпоху раннего интернета, что внутренние регламенты запрещают передавать клиентские данные в сторонние сервисы, а корпоративная сеть фильтрует обращения к внешним интерфейсам. Проектирование потоков данных, очистка и нормализация исторических записей, разработка внутреннего шлюза для изоляции персональной информации — всё это заняло кратно больше времени, чем первоначальная оценка. Если вы планируете внедрение, умножьте смету на три с учетом железа и добавьте четыре месяца. Будете близки к истине.

Отдельная тема — качество данных. Искусственный интеллект работает ровно настолько хорошо, насколько качественны данные, которыми его кормят. Мусор на входе дает мусор на выходе — эта истина стара, как программирование, но почему-то каждый раз открывается заново.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР: САМАЯ СЛОЖНАЯ ИНТЕГРАЦИЯ

Технические проблемы решаемы — это вопрос ресурсов и времени. Человеческое сопротивление — отдельный вид искусства.

Самым продуктивным оказалось не убеждение, а совместная работа: взять реальную задачу конкретного отдела, решить ее с помощью нового инструмента и отдать коллеге самому убедиться в результате. После этого он становится лучшим проводником изменений в своем подразделении.

РЕГУЛЯТОРНАЯ СРЕДА — ИГРАЕМ ПО ПРАВИЛАМ, КОТОРЫЕ ЕЩЕ ПИШУТСЯ

Здесь начинается самое интересное. Российское законодательство в области применения искусственного интеллекта находится в стадии активного формирования, что означает: правила меняются быстрее, чем успевают адаптироваться корпоративные юридические службы. Для брокерской деятельности принципиальными остаются несколько ограничений. В первую очередь — работа с персональными данными, требующая максимальной надежности и защищенности. Мы пошли путем полной локализации, то есть разворачивания моделей на своем железе. Тут две стороны медали: с одной стороны, это дорогостоящая инвестиция и на начальных этапах не каждая компания готова вложиться, но с другой — это дает полную автономность и независимость от внешнего контура, что даже ментально предоставляет чувство стабильности. Второй важный момент касается взаимодействия с клиентами. Банк России пристально следит за тем, чтобы автоматизированные системы не принимали инвестиционные решения без надлежащего контроля со стороны человека. Любой инструмент, который можно квалифицировать как средство инвестиционного консультирования, немедленно попадает в зону регуляторного внимания. Мы тщательно разграничиваем: система помогает аналитику, но не заменяет его суждение. Это не просто красивая формулировка — это обязательное требование к архитектуре процессов.

Российское законодательство в области применения искусственного интеллекта находится в стадии активного формирования

МИФ ТРЕТИЙ: «ДОСТАТОЧНО ОДИН РАЗ НАСТРОИТЬ»

Последнее заблуждение, которое требует внимания, касается сопровождения. Многие представляют внедрение как проект с четким финалом: настроили, запустили, забыли. Это не так. Модели устаревают. Регуляторная среда меняется. Внутренние процессы эволюционируют. Качество данных деградирует, если за ним не следить. Сотрудники находят новые способы использования инструментов — хорошие и не очень. Всё это требует постоянного внимания, итерационного улучшения и, что важно, выделенной команды, которая понимает и бизнес-контекст, и технические основы.

Что можно однозначно сказать о всей этой истории? Искусственный интеллект в брокерской компании — это реально работающий инструмент, который дает измеримый результат при условии трезвого взгляда на его возможности. Он не оракул, не замена экспертизе и не волшебная кнопка сокращения издержек. Он — очень способный, иногда самонадеянный, требующий постоянного надзора помощник.

Дмитрий АЛЕКСАНДРОВ,
руководитель управления аналитических исследований, «АВИ Кэпитал»

ИИ В ФИНАНСОВОЙ АНАЛИТИКЕ: ЧТО УЖЕ РАБОТАЕТ, ГДЕ ОН ЛОМАЕТСЯ И ЧЕМ ЭТО ЗАКОНЧИТСЯ ДЛЯ ИНВЕСТОРА?

За последние два года языковые модели превратились из выставочного экспоната в рабочий инструмент аналитика. Обсуждать «ИИ в аналитике» — абстрактно, бессмысленно — всё решает связка: модель, retrieval* (здесь и далее ко всем терминам, отмеченным звездочкой, даны расшифровки в глоссарии в Таблицы 1), структурированные выходы и контур проверки. Там, где эта инженерия собрана, ИИ реально экономит человеко-часы. Там, где ее нет, он генерирует уверенно звучащий шум. ИИ закрывает рутину и ускоряет первичную обработку данных, но принятие решений по-прежнему остается за человеком, и в ближайшие несколько лет эта граница вряд ли исчезнет.

ЧТО РЕАЛЬНО РАБОТАЕТ

Во-первых, извлечение и нормализация структурированной информации: разбор МСФО- и РСБУ-отчетностей, унификация пресс-релизов, вытаскивание covenant*-параметров из проспектов облигаций, сравнение ESG*-раскрытий. Вторая зрелая ниша — новостной скрининг*, сентимент*-метки, разметка по эмитенту и фактору. Третья — драфты записок и препроцессинг* для quant*-моделей. Для сектора, где ценятся скорость и охват, это уже дало заметный прирост производительности. Общее у успешных кейсов одно: eval-наборы* (грубо — фиксированные тестовые выборки, на которых регулярно прогоняют модель и сравнивают ее ответы с эталоном) и регулярный QA* (постоянный процесс проверки модели на качество ответа, в том числе, чтобы отлавливать model drift*). Без них преимущество ИИ исчезает под весом точечных ошибок.

ГДЕ СИСТЕМНО БЫВАЮТ ПРОБЛЕМЫ

Проблемы, тем не менее, никуда не делись. Первая и главная — фактическая надежность. Арифметика и масштаб единиц — классическая зона провала: токенизация чисел не гарантирует корректности даже простых delta-расчетов*, модель уверенно путает тысячи с миллионами, rub* с usd*, quarterly* с annualized*. Второе — пока плохо масштабируется работа со сносками, а в отчетности вес раскрытия в примечаниях нередко превышает вес основной таблицы. В-третьих, модели без tool-use* имитируют вычисления, а не выполняют их; модели без привязки к верифицированному источнику и с истекшим knowledge cutoff* выдают фактологически уверенные, но ложные утверждения — эффект, хорошо известный как confident hallucination*. Про model drift* уже упомянули. К этому добавляются регуляторные требования к раскрытию источников и ответственности — они скорее всего будут ужесточаться.

ТОНКИЕ РИСКИ ВТОРОГО ПОРЯДКА

Возможное смещение при расчете/извлечении из отчетностей значений маржинальности, путаница scale-факторов* в сносках, что транслируется в ложные earnings-surprise*. Смешение тикеров после корпоративных событий или сведения данных с разных площадок, что при автоматическом исполнении ордеров дает прямой операционный убыток. ИИ-советники могут создавать диверсифицированные портфели, подстраиваясь под профиль риска клиента, вопрос только в правильности профилирования и излишней синхронизации, которая может воспроизвести просто очередную версию «народного портфеля». С другой стороны, а почему при простейшем «лобовом» применении ИИ должно получиться что-то другое? Плохо, однако, что розничный пользователь будет переоценивать степень персонализации ответа. При этом возможность выявлять корреляции всего со всем, обнаруживая неочевидные и скрытые зависимости, причем проводя глубокую и многостороннюю статистическую обработку, но без базовых представлений как о статистике, так и об экономике, рынке, природе активов, есть риски получать самые причудливые ошибочные логические выводы.

Кроме того, если значимая часть рынка работает со схожим набором foundation-моделей* на одних и тех же корпусах, возникает дополнительный канал синхронизации сделок; в стрессовые периоды это расширяет амплитуду движений в низколиквидных (и не только) активах и заставляет вспомнить о Flash-Crash* 2011 года в США на основе алгостратегий.

Особо опасная история — prompt injection* через внешние документы, утечки контекста между клиентами в мультитенантных средах и воспроизводимость: вывод LLM* без фиксированного seed* и снапшота*.

РЕГУЛЯТОРНЫЙ КОНТУР

Требования к раскрытию использования ИИ, проверке данных и распределению ответственности между провайдером модели и брокером, по факту, будут довольно жестко формализованы, видимо, на горизонте двух-трех лет. Сложность, а иногда и невозможность логической интерпретации принципа принятия решений нейросетями вызывает недоверие у регуляторов к таким «черным ящикам», так что регуляторика будет усложняться, а прямой допуск ИИ к принятию решений — ограничиваться. Общая логика Банка России обозначена в докладе 2023 года: риск-ориентированный подход, требование объяснимости моделей, обязательный человеческий контроль над сделками, валидация данных, контроль за использованием ИИ в скоринге*, маркетинге, эдвайзинге*. Для брокеров и УК это означает три конкретные вещи. Первое — внутренние политики использования ИИ с назначенным ответственным, журналированием промптов и версий моделей. Второе — обязательное раскрытие клиенту, что рекомендация, сводка или ответ сгенерированы ИИ с разграничением investment advice* и информационного сервиса. Третье — требования к data residency* и изоляции данных, фактически закрывающие использование публичных облачных моделей для чувствительных корпоративных контуров.

КОНТУР НОВЫХ ПРОДУКТОВ

Перспективы выглядят как последовательная эволюция продуктов. Массовому инвестору будут все более доступны встроенные в брокерские приложения ассистенты: контекстное объяснение новостного фона по бумагам в портфеле, сводки отчетностей с подсветкой изменений к консенсусу, подсказки по диверсификации и налоговой оптимизации. Корпоративный сегмент — это агентные решения для due-diligence*, комплаенса* и санкционного скрининга, интеграции с ERP/TMS*, внутренние

Термин	Краткая расшифровка
Retrieval	поиск и извлечение релевантных данных из источников
Covenant	договорное ограничение или обязательство заемщика
ESG	экологические, социальные и управленческие факторы
Quant-модели	количественные модели на основе данных и статистики
Eval-наборы	тестовые выборки для проверки качества модели
QA	контроль качества
Model drift	ухудшение модели из-за изменения данных или среды
Delta-расчеты	расчеты изменений показателя
Rub	рубли
Usd	доллары США
Quarterly	квартальное значение
Annualized	значение, приведенное к годовому выражению
Tool-use	использование внешних инструментов моделью
Knowledge cutoff	дата, после которой модель не знает новых данных
Confident hallucination	уверенно сформулированное, но ложное утверждение модели
Scale-факторы	коэффициенты масштаба, например: тысячи или миллионы
Earnings-surprise	неожиданное отклонение финансового результата от ожиданий
Foundation-модель	базовая универсальная модель, обученная на широком корпусе данных
Flash Crash	резкий краткосрочный обвал рынка
Prompt injection	внедрение вредоносных инструкций в запрос или документ
LLM	большая языковая модель
Seed	начальное значение генератора случайности
Снапшот	снимок состояния системы или модели
Investment advice	инвестиционная рекомендация
Data residency	требование хранить данные в определенной юрисдикции
Due diligence	комплексная проверка перед сделкой
ERP	система управления ресурсами предприятия
TMS	казначейская система управления ликвидностью и платежами
Knowledge-ассистент	ассистент для поиска и обработки корпоративных знаний
Fine-tune	дообучение модели на специализированных данных
Inference	вычислительный вывод модели при ответе на запрос
Persistent-память	долговременное сохранение контекста о пользователе или задаче
Evaluated-агенты	агенты, прошедшие регулярную проверку качества
SLA	соглашение об уровне сервиса
MLOps	эксплуатация и мониторинг моделей машинного обучения
Скрининг	быстрый первичный отбор или проверка
Сентимент	тональность сообщения или новости
Препроцессинг	предварительная обработка данных
Комплаенс	контроль соблюдения правил и требований
Скоринг	автоматизированная система оценки финансовой надежности и платежеспособности клиента
Эдвайзинг	консультационный сервис или рекомендации клиенту
Мультитенантная среда	общая инфраструктура для нескольких клиентов с изоляцией данных

Таблица 1
Глоссарий используемых терминов

knowledge-ассистенты* на изолированных моделях с доменным fine-tune*. Вероятным выглядит и сегмент вертикальных моделей, обученных на узких корпусах — отраслевых отчетах, регуляторных базах, историческом макросе, — с лицензированием под контуры конкретных управляющих. Отдельный блок — агентные решения, способные выполнять последовательности задач в согласованном контуре под надзором эксперта.

ЭКОНОМИКА ПЛАТНОСТИ И ПЕРИОДИЧЕСКАЯ СМЕНА ФОКУСА

Сформируется, видимо, двухслойная модель. В бесплатный сегмент уйдут (приняв на себя маркетинговые функции) задачи, где себестоимость inference* стремится к минимуму: пересказы, формальные расчеты, перевод раскрытий, базовый скрининг. Платным останется то, что требует уникального подхода, — верифицированные данные, интеграция с корпоративными системами, persistent*-память о клиенте, evaluated*-агенты с SLA* на качество и ответственность за вывод. Соответственно, ценность массовой обезличенной аналитики будет снижаться, а премия за авторскую экспертизу и качество исходных данных — расти. При этом если сначала клиенту (как розничному, так и корпоративному) будет интересно «поиграть» в моделирование портфелей и стратегий, то затем последует рост спроса на действительно расширенный и глубокий анализ, что сместит фокус продаж и повлияет на формат и цены продуктов.

Таким образом, ИИ в ближайшие годы — не замена аналитика, а инженерная надстройка, усилитель-ускоритель аналитического процесса и бизнеса. Выигрывать будут те участники рынка, которые относятся к нему как к элементу инфраструктуры с собственным регламентом эксплуатации, тестированием и зонами ответственности. Команда аналитиков должна при этом обладать и свойствами инженеров данных, поддерживающих полноценный MLOps*-контур под нужную регулярность обновлений.

Кстати, один абзац этой статьи полностью написан ИИ, без правок, но в стилистике автора. Угадаете, какой?