ТЗ: Антифрод-система для проп-трейдинговой платформы

Nov 16, 2026 ·

1. Общие сведения

YouTrade ищет исполнителя, который разработает систему автоматического выявления мошенничества и запрещённых торговых практик на проп-трейдинговой платформе.

Параметр	Значение
Заказчик	ТОО «Kubayev Capital» (бренд YouTrade, youtradeprop.com), Казахстан
Название задачи	Антифрод-система для проп-трейдинговой платформы на базе ИИ
Тип задачи	ICT-задача
Отрасль	Финтех, проп-трейдинг (оценочные и финансируемые торговые счета)
Предпочтительные технологии	Нейротехнологии и искусственный интеллект; технологии цифровой безопасности; обработка больших данных
Тип продукта	Программное обеспечение / информационная система (веб-интерфейс + API)
Статус продукта	Идея: правила и ручной процесс проверки есть, автоматизации нет
Торговая платформа заказчика	Match-Trader (торговля + CRM)

2. Цель и описание задачи

Цель — система, которая по данным платформы сама находит нарушения правил и связанные счета, оценивает риск каждого трейдера и готовит риск-менеджеру доказательную базу до выплаты. Решение о блокировке или отказе в выплате остаётся за человеком; система находит, объясняет и ранжирует.

Исполнитель должен:

1. Собрать и нормализовать данные о сделках, счетах, клиентах, платежах и входах в единое хранилище.
2. Реализовать конфигурируемый движок правил для нарушений с чёткими критериями (новости, маржа, хеджирование).

3. Построить граф связей между клиентами и счетами для выявления мультиаккаунтинга и групповой торговли.
4. Обучить ML-модели для практик без чёткого порога: боты, копирование сигналов, арбитраж задержек, аномалии.
5. Считать риск-скор счёта и группы связанных счетов почти в реальном времени и обязательно перед каждой выплатой.
6. Дать риск-менеджеру веб-интерфейс: алерты, карточки расследований, историю нарушений, отчёты.
7. Интегрировать систему в процесс выплат и CRM через API.

Результат: работающая система, развёрнутая в инфраструктуре заказчика, с исходным кодом, обученными моделями и документацией.

3. Описание проблемы

Часть трейдеров проходит оценку и получает выплаты не за счёт навыка, а за счёт обхода правил, а выявляем мы это вручную и с опозданием. Каждая пропущенная схема — это прямая выплата из средств компании и искажение статистики для честных трейдеров.

Контекст. YouTrade — проп-трейдинговая компания из Казахстана. Трейдер покупает челлендж (оценочный счёт), проходит этапы и получает финансируемый счёт с разделом прибыли. Клиенты — из Казахстана, России, Украины, Узбекистана, Польши и стран ЕС.

Как проверяем сейчас. Риск-менеджер выгружает данные из CRM, вручную сверяет сделки с новостным календарём, ищет похожие счета и проверяет, нарушал ли трейдер раньше. Автоматика платформы покрывает только лимиты просадки (дневная 5%, максимальная 6–8% в зависимости от продукта), но не поведенческие нарушения.

Что не работает:

- **Не видны связанные счета.** Мультиаккаунты на разные имена, email и карты вручную не сопоставить, а именно на них строятся хеджирование между счетами и групповая торговля.
- **Проверка выборочная.** Не каждая выплата проходит полную проверку; результат зависит от опыта и внимания конкретного сотрудника.
- **Нет единой истории нарушений.** Повторное нарушение (второе soft-нарушение = блокировка) легко пропустить, особенно если трейдер вернулся под новым счётом.
- **Сложные схемы не ловятся правилами.** Боты, копирование сигналов и арбитраж задержек требуют анализа поведения, а не простого порога.
- **Ручная проверка не масштабируется.** Рост числа трейдеров требует пропорционального роста риск-команды.

4. Каталог нарушений

Система должна выявлять 10 типов нарушений и риск-паттернов. Категория задаёт последствия по правилам YouTrade: **Hard** — немедленная блокировка; **Soft** — первое нарушение = предупреждение, второе = блокировка; **Риск-паттерн** — не нарушение сам по себе, но повышает риск-скор и требует проверки.

#	Нарушение	Категория	Признаки для детекции	Метод
1	Хеджирование между счетами	Hard	Противоположные позиции по одному инструменту на разных счетах, открытые в близкое время со схожим объёмом; один счёт сливается, другой проходит оценку	Правило + граф связей
2	Мультиаккаунтинг	Hard	Общие IP или подсети, отпечаток устройства, платёжные реквизиты, похожие email, данные KYC, адрес, совпадающее время входов	Граф связей, entity resolution
3	Групповая торговля и копирование сигналов	Hard	Синхронные входы и выходы у формально не связанных трейдеров, одинаковые инструменты, SL/TP и размеры лотов	ML: кластеризация и похожесть торговых последовательностей
4	Торговые роботы (советники, скрипты)	Hard	Равные интервалы между ордерами, нечеловеческая скорость реакции, круглосуточная активность без пауз, одинаковые объёмы и модификации ордеров	ML-классификатор поведения
5	Арбитраж задержек и эксплуатация котировок	Риск-паттерн (категорию в правилах уточняет заказчик)	Прибыльные сделки длительностью секунды, вход в момент расхождения цены с эталонным фидом, аномально высокий винрейт на сверхкоротких сделках	Сверка с эталонными котировками + ML
6	Торговля на «красных» новостях	Soft	Открытие или закрытие позиции в окне ±3 минуты (UTC) вокруг важных событий (CPI, NFP и др.) по связанным инструментам	Правило + экономический календарь

#	Нарушение	Категория	Признаки для детекции	Метод
7	Использование более 70% маржи	Soft	Загрузка маржи выше 70% в любой момент торговли	Правило
8	Злоупотребление промокодами и партнёрской программой	Риск-паттерн	Партнёр покупает челленджи по своему промокоду через связанные аккаунты; многократное использование скидок одним человеком	Граф связей + правила
9	Платёжный фрод	Риск-паттерн	Оплата чужой картой, одни реквизиты на нескольких клиентов, несовпадение страны карты, IP и KYC, чарджбэки после выплаты	Правила + граф связей
10	Стратегии «на удачу»	Риск-паттерн	Прохождение этапа одной-двумя сделками максимальным объёмом; массовая покупка челленджей с одинаковым паттерном	ML: аномалии и профиль риска

Перечень не закрытый: заказчик должен иметь возможность добавлять новые правила и менять пороги (окна времени, процент маржи, список событий) без участия разработчиков.

5. Исходные данные и интеграции

Основной источник — торговая платформа и CRM Match-Trader; остальные источники усиливают поиск связей и платёжного фрода. Формат и способ доступа (API или регулярные выгрузки) согласуются на первом этапе.

Источник	Данные	Зачем нужны
Торговая платформа Match-Trader	Сделки и ордера (время до миллисекунд, инструмент, направление, объём, цены, SL/TP, модификации), позиции, баланс и маржа	Все торговые нарушения (п. 1, 3–7, 10)
CRM Match-Trader	Клиенты, счета (Login), челленджи и их этапы, статусы, страна, KYC-статус, промокоды и партнёры	Привязка счетов к людям, мультиаккаунтинг, промокоды
Журналы входов и сессий	IP, геолокация, user-agent, отпечаток устройства, время сессий	Граф связей. Если платформа их не отдаёт, исполнитель предлагает

Источник	Данные	Зачем нужны
		сбор на сайте и в личном кабинете
Платёжные провайдеры	Покупки челленджей, запросы и факты выплат, маскированные реквизиты (BIN, страна карты, кошелёк), чарджбэки	Платёжный фрод, связи по реквизитам, проверка перед выплатой
Эталонные котировки	Тиковые цены поставщика ликвидности или независимого источника	Арбитраж задержек (п. 5)
Экономический календарь	Важные события, время в UTC, валюта и связанные инструменты	Торговля на новостях (п. 6)
История нарушений заказчика	Прошлые кейсы, принятые решения, предупреждения и блокировки	Разметка для обучения ML и учёт повторных нарушений

Объём данных (число счетов, сделок в сутки, глубина истории) и обезличенная выборка для оценки передаются исполнителю после подписания NDA.

6. Функциональные требования

Система состоит из десяти модулей. Ключевой сценарий — проверка перед выплатой (модуль 6): ни одна выплата не уходит без автоматического отчёта о риске.

1. **Сбор и нормализация данных**
   - Инкрементальная загрузка из источников раздела 5: сделки — почти в реальном времени, справочники — по расписанию.
   - Единая модель данных: клиент → счета → сделки → платежи → сессии; всё время в UTC.
   - Дедупликация, контроль полноты и оповещение при сбое загрузки.
2. **Движок правил**
   - Правила с параметрами (окна времени, пороги, списки инструментов и событий), которые риск-менеджер меняет через интерфейс.
   - Проверка нового правила на исторических данных до включения: сколько сработало бы и на ком.
   - Версионирование: каждое срабатывание хранит, какая версия правила его вызвала.
3. **Граф связей**
   - Объединение клиентов и счетов в кластеры по общим атрибутам (IP, устройство, реквизиты, KYC, поведение) с весом каждой связи.
   - Визуализация графа с объяснением, почему два счёта связаны.
   - Ручное подтверждение или разрыв связи (например, семья или офис с общим IP).
4. **ML-модели**

- Детекция ботов, поиск синхронной торговли и копирования, арбитраж задержек, аномалии профиля.
- Объяснимость: к каждому срабатыванию — главные признаки, которые на него повлияли.
- Обратная связь: решения риск-менеджера (подтвердил или ложное срабатывание) идут в переобучение.
- Мониторинг качества моделей и дрейфа данных.

5. **Риск-скоринг**
   - Скор 0–100 для счёта, клиента и кластера связанных счетов, с уровнями «низкий / средний / высокий / критический».
   - Пересчёт при новых сделках, переходе на следующий этап челленджа и запросе выплаты.
6. **Проверка перед выплатой**
   - При запросе выплаты система формирует отчёт: нарушения, связанные счета, риск-скор и рекомендацию «одобрить / проверить вручную / отклонить».
   - Итоговое решение принимает сотрудник; система фиксирует, кто и почему его принял.
7. **Карточка расследования (кейс)**
   - Обязательные поля: номер счёта (Login), email, статус счёта, время нарушения в UTC, событие (CPI, NFP и т.п.), количество ордеров и предыдущие нарушения клиента и его кластера.
   - Доказательства: график сделок на цене, таблица совпадений между счетами, фрагмент графа связей.
   - Статусы кейса, назначение ответственного, комментарии, решение.
   - Шаблоны уведомлений трейдеру с автовыбором по истории: первое предупреждение, повторное нарушение, блокировка.
8. **Алерты**
   - Уведомления в веб-интерфейсе, Telegram и email с приоритетом по риску.
   - Группировка повторяющихся срабатываний по одному счёту, чтобы не засорять канал.
9. **Дашборд и отчётность**
   - Нарушения по типам и периодам, сумма остановленных выплат, доля ложных срабатываний, время обработки кейса.
   - Экспорт в CSV и PDF.
10. **API, роли и аудит**
    - REST API: риск-скор счёта, статус проверки выплаты, webhook в CRM.
    - Роли: администратор, риск-менеджер, финансы (только статус выплат), наблюдатель.
    - Журнал всех действий пользователей и изменений правил.

7. Нефункциональные требования

Главное требование — объяснимость: ни одно срабатывание не может быть «чёрным ящиком», потому что решение о блокировке должно быть обосновано перед трейдером. Целевые значения ниже уточняются с исполнителем.

- **Скорость.** Алерт по правилу — не позднее 1 минуты после сделки; отчёт перед выплатой — до 30 секунд; пересчёт ML-моделей — не реже раза в сутки.
- **Масштабируемость.** Рост числа счетов и сделок в 10 раз без переделки архитектуры.
- **Доступность.** Не ниже 99,5% в месяц; сбой антифрода не должен останавливать работу торговой платформы.
- **Безопасность.** Шифрование данных при хранении и передаче, ролевой доступ, двухфакторная аутентификация, журнал аудита.
- **Персональные данные.** Обработка в соответствии с Законом РК «О персональных данных и их защите»; минимизация данных, псевдонимизация в ML-контуре, полные номера карт не хранятся.
- **Размещение.** В облаке или на серверах заказчика; данные не покидают контур заказчика. Развёртывание в контейнерах (Docker).
- **Объяснимость.** У каждого срабатывания — причина простым языком и ссылки на конкретные сделки.
- **Языки интерфейса.** Русский и английский; шаблоны уведомлений трейдерам — на русском и английском.
- **Документация.** Архитектура, описание API, руководство пользователя, описание моделей и признаков, инструкция по развёртыванию.

10. Критерии приёмки и целевые метрики

Система принимается по итогам 4-недельного пилота, в котором она работает параллельно с ручной проверкой, а результаты сравниваются. Целевые значения фиксируются в договоре с исполнителем.

Метрика	Цель	Как измеряется
Полнота по Hard-нарушениям (recall)	≥ 90%	Доля исторических подтверждённых кейсов, которые система находит сама
Точность алертов (precision)	≥ 70%	Доля алертов, подтверждённых риск-менеджером на пилоте
Покрытие каталога	10 из 10 типов	Каждый тип из раздела 4 реализован и проверен на тестовых случаях
Проверка выплат	100%	Доля запросов на выплату с автоматическим отчётом о риске

Метрика	Цель	Как измеряется
Время расследования кейса	В 3 раза меньше	Замер до и после внедрения на одинаковых типах кейсов
Объяснимость	100%	У каждого срабатывания есть причина и список сделок-доказательств
Скорость	≤ 1 мин / ≤ 30 с	Алерт после сделки / отчёт перед выплатой, 95-й перцентиль
Доступность	≥ 99,5%	Мониторинг за месяц пилота