

Т3: Система мониторинга транзакций и выявления мошенничества в реальном времени

1. Общие сведения

Monexsol ищет технологическое решение для мониторинга транзакций и выявления мошенничества в реальном времени для своего мобильного платёжного приложения. Документ является приложением к технологической задаче на портале astanahub.com и служит для сбора предложений.

Параметр	Значение
Заказчик	Monexsol ltd.
Наименование	Система мониторинга транзакций и выявления мошенничества в реальном времени для мобильного платёжного приложения
Основание	Технологическая задача на портале astanahub.com
Целевой рынок	Страны СНГ
Стадия продукта заказчика	MVP, подготовка к коммерческому запуску
Статус документа	Сбор предложений, не является офертой
Контактное лицо	Указано в карточке задачи на портале

2. Назначение и цели

Решение должно оценивать риск каждой операции до её проведения и останавливать мошеннические операции без лишних помех для добросовестных клиентов.

1. Запустить продукт с работающим контуром мониторинга транзакций с первого дня коммерческой эксплуатации.
2. Снизить прямые финансовые потери от мошенничества и обязательства по возмещению ущерба клиентам.
3. Обеспечить соответствие требованиям регуляторов стран присутствия и банков-партнёров к мониторингу операций и ПОД/ФТ.
4. Сократить сроки и затраты по сравнению с собственной разработкой антифрод-системы.

В границы задачи входят мониторинг операций и событий учётной записи, антифрод-правила и скоринг, мониторинг операций по типологиям ПОД/ФТ и разбор инцидентов. Проверка по санкционным спискам и спискам публичных должностных лиц - опциональный модуль, его наличие указывается в предложении.

В границы задачи не входят идентификация клиента при регистрации (KYC), аутентификация и дополнительное подтверждение операций, процессинг платежей и направление отчётности в уполномоченные органы финансового мониторинга. Эти функции остаются на стороне заказчика и его финансовых партнёров.

3. Характеристика продукта заказчика

Продукт - мобильное платёжное приложение для частных лиц и бизнеса, ориентированное на рынок стран СНГ.

Параметр	Описание
Функции	P2P-переводы, оплата услуг, электронный кошелёк, QR-платежи, приём платежей для бизнеса
Плановый объём операций	Ориентировочно до 2 млн операций в месяц на первом этапе с ростом до 10 млн
Расчётная нагрузка на антифрод-контур	До 100 событий в секунду в пике с ростом до 500
Юрисдикции	Несколько стран СНГ с разными валютами и регуляторными требованиями; перечень стран первой очереди сообщается выбранным участникам
Исторические данные о мошенничестве	Отсутствуют (продукт до коммерческого запуска)
События для оценки риска	Платежи и переводы, входы в приложение, привязка карт, смена устройства и данных учётной записи

4. Сценарии мошенничества

Решение должно покрывать шесть сценариев, типичных для платёжных приложений.

Перечень сигналов - ориентир, а не закрытый список.

Сценарий	Суть	Примеры сигналов
Социальная инженерия	Клиента убеждают самостоятельно перевести средства мошеннику	Первый перевод новому получателю, сумма выше обычной, серия операций за короткое время
Захват учётной записи	Мошенник получает доступ к аккаунту и выводит средства	Вход с нового устройства, смена номера или пароля перед переводом, признаки эмулятора
Скомпрометированные карты	Привязка и проверка чужих карт	Много карт на одно устройство, серия мелких пробных операций
Дропперские схемы	Транзит похищенных средств через счета подставных лиц	Быстрый вывод входящих средств, много отправителей на одного получателя
Мультиаккаунты	Злоупотребление бонусными	Одно устройство или одни реквизиты у нескольких учётных

Сценарий	Суть	Примеры сигналов
	механиками	записей
Получатель в стоп-листе	Перевод лицу, уже внесённому в списки мошенников	Совпадение с национальными или внутренними стоп-листами

5. Функциональные требования

Решение должно выполнять девять функций. Пункты 1–7 обязательны для PoC, пункты 8–9 - для пилота.

1. Оценка риска операции в реальном времени до её проведения с результатом: пропустить / запросить дополнительное подтверждение / отклонить. Дополнительное подтверждение выполняет приложение заказчика.
2. Сочетание настраиваемых правил (лимиты, частота операций, аномалии по сумме, времени и географии) и моделей машинного обучения на основе поведения пользователя. Правила меняются аналитиком заказчика без участия разработчиков.
3. Анализ признаков устройства и сессии для защиты от захвата учётной записи: смена устройства, эмуляторы, модифицированные ОС, аномалии входа.
4. Выявление дропперских схем и транзитных счетов в P2P-переводах, а также злоупотребления бонусными механиками (мультиаккаунты).
5. Модуль разбора инцидентов: очередь подозрительных операций, рабочее место аналитика, журнал решений с аудиторским следом.
6. Объяснимость решений: причина срабатывания по каждой операции для разбора обращений клиентов.
7. Работа без исторических данных заказчика (холодный старт): преднастроенные правила и модели с последующим дообучением на данных заказчика.
8. Загрузка и применение внутренних стоп-листов и списков, которые заказчик получает от национальных антифрод-систем и регуляторов стран присутствия (например, Антифрод-центра Национального Банка РК).
9. Поддержка нескольких юрисдикций и валют: отдельные правила, лимиты и списки для каждой страны присутствия.

6. Нефункциональные требования

Проверка стоит в синхронной цепочке платежа, поэтому ключевые требования - скорость ответа и предсказуемое поведение при сбое. Нагрузка рассчитана с запасом на пятикратный рост аудитории.

Показатель	Требование
Время принятия решения	Не более 200 мс для 95% операций и не более 500 мс для 99% операций. Измеряется как время ответа API на стороне заказчика при размещении в одном регионе
Пропускная способность	Не менее 100 событий в секунду в пике с горизонтальным масштабированием до 500 событий в секунду

Показатель	Требование
Доступность	Не ниже 99,9% за календарный месяц, без учёта согласованных окон обслуживания
Поведение при сбое	При недоступности или превышении времени ответа - обработка по резервной политике: автоматический пропуск операций до установленного лимита суммы, отклонение или отложенная проверка операций выше лимита. Лимиты настраивает заказчик
Размещение	Облако или собственная инфраструктура с возможностью развёртывания в нескольких странах для соблюдения требований о локализации персональных данных

7. Интеграция, данные и информационная безопасность

Интеграция должна требовать минимальных доработок на стороне заказчика, а данные клиентов - обрабатываться по законодательству стран присутствия.

- **API.** Синхронный REST API для оценки операции; вебхуки для асинхронных событий (результаты разбора, смена статусов); документация в формате OpenAPI; тестовая среда для интеграции.
- **Архитектура.** Совместимость с микросервисной архитектурой, SDK или библиотека для сбора признаков устройства в мобильном приложении (iOS, Android).
- **Списки.** Импорт внутренних стоп-листов и списков, полученных заказчиком, через API или файловый обмен с автоматическим обновлением.
- **Данные.** Заказчик передаёт минимально необходимый набор данных об операции, устройстве и сессии. Полные номера карт не передаются: используются токены или хеши, BIN и последние 4 цифры. Решение поддерживает псевдонимизацию персональных данных.
- **Персональные данные.** Обработка исполнителем - только на основании соглашения об обработке данных и в соответствии с законодательством стран присутствия, включая требования к трансграничной передаче.
- **Безопасность.** Шифрование при передаче (TLS 1.2 и выше) и хранении, ролевая модель доступа, журналирование действий пользователей и изменений правил. Сертификация PCI DSS, ISO/IEC 27001 или эквивалентная - преимущество.
- **Отчётность.** Выгрузка отчётов по инцидентам и срабатываниям для внутреннего контроля и запросов регуляторов.

8. Этапы взаимодействия и критерии приёмки

Сотрудничество с выбранным участником предполагается в два этапа; каждый следующий начинается только после успешного завершения предыдущего.

1. **Этап 1 - консультация и PoC.** Архитектурная консультация и проверка в тестовой среде на сценариях раздела 4 и эталонных данных участника.
2. **Этап 2 - пилот.** Работа на ограниченном потоке реальных операций после коммерческого запуска не менее 2 месяцев - срок, необходимый для достоверного измерения показателей.

Модель сотрудничества (подписка SaaS, лицензия или совместная разработка), сроки и стоимость определяются по итогам рассмотрения предложений.

РоС принимается при выполнении четырёх условий; все они проверяются без исторических данных заказчика:

Условие РоС	Как проверяется
Выявление всех шести сценариев раздела 4	Прогон тестовых сценариев, подготовленных заказчиком совместно с участником
Время принятия решения не более 200 мс для 95% операций	Нагрузочный тест при 100 событиях в секунду
Интеграция с тестовой средой заказчика	Вызов оценки операции и получение вебхуков
Объяснимость	Причина срабатывания по каждой операции тестового набора

Пилот считается успешным при достижении трёх показателей на реальных операциях. Подтверждёнными случаями мошенничества считаются обращения клиентов, данные финансовых партнёров и национальных антифрод-систем.

Показатель пилота	Целевое значение
Выявление подтверждённых мошеннических операций	Не менее 80%
Ложные срабатывания	Не более 0,5% легитимных операций
Автоматизация решений	Не менее 99,9% операций решаются автоматически, на ручной разбор - не более 0,1%

9. Разграничение ответственности и поддержка

Решение по операции принимает система исполнителя, а исполняет его приложение заказчика.

Зона	Заказчик	Исполнитель
Данные об операциях, устройстве и сессии	Формирует и передаёт через API	Принимает и проверяет полноту
Решение по операции	Исполняет в приложении, включая дополнительное подтверждение	Возвращает решение и причину срабатывания
Правила и лимиты	Настраивает аналитик заказчика	Предоставляет инструмент и обучение
Модели машинного обучения	Передаёт результаты разбора инцидентов	Обучает, контролирует качество, переобучает

Зона	Заказчик	Исполнитель
Разбор инцидентов	Ведёт аналитик заказчика	Предоставляет рабочее место и журнал
Списки национальных антифрод-систем	Получает при наличии доступа к этим системам	Загружает и применяет
Сбои сервиса	Применяет резервную политику (раздел 6)	Обеспечивает доступность и устраняет сбои

Поддержка исполнителя: критические инциденты (недоступность или массовые ошибки оценки) - круглосуточно, время реакции не более 30 минут; прочие обращения - в рабочее время, ответ не позднее следующего рабочего дня.

10. Требования к предложению участника

Предложение направляется через форму отклика на портале astanahub.com и должно содержать восемь блоков:

1. Описание решения и его архитектуры; готовый продукт или разработка под заказчика.
2. Матрица соответствия сценариям раздела 4 и требованиям раздела 5: выполняется / частично / не выполняется.
3. Подтверждение показателей раздела 6 (задержка, нагрузка, доступность).
4. Варианты размещения и подход к локализации персональных данных в странах СНГ.
5. Опыт внедрений в банках, платёжных или финтех-компаниях; кейсы в СНГ - преимущество.
6. Условия PoC: сроки, требуемые данные, стоимость или бесплатный формат.
7. Модель и ориентировочная стоимость коммерческого использования.
8. Сроки и трудозатраты интеграции со стороны заказчика.

Предложения принимаются на русском или английском языке в течение срока публикации задачи на портале. Вопросы по ТЗ направляются контактному лицу, указанному в карточке задачи. Заказчик рассматривает предложения в течение 10 рабочих дней после окончания приёма и сообщает результат каждому участнику через портал.

11. Критерии оценки предложений

Предложения оцениваются по пяти критериям; наибольший вес имеет покрытие функциональных требований.

Критерий	Вес
Соответствие функциональным требованиям и сценариям (разделы 4–5)	30%
Нефункциональные показатели (раздел 6)	20%
Совокупная стоимость владения, включая условия PoC	20%
Опыт внедрений в финансовом секторе СНГ	15%
Сроки и простота интеграции	15%

Предложения, не покрывающие пункты 1–7 раздела 5, не оцениваются.

12. Ограничения и оговорки

Публикация задачи и настоящее ТЗ служат сбору предложений и не создают обязательств ни для одной из сторон.

- Публикация не является офертой. Заказчик рассматривает решения по собственным критериям и вправе не выбрать ни одно из них.
- На этапе сбора предложений заказчик не передаёт и не запрашивает конфиденциальную информацию. Обмен ей возможен только после подписания соглашения о конфиденциальности.
- Стоимость, сроки и модель сотрудничества определяются по итогам рассмотрения предложений и фиксируются отдельным договором.
- Права на результаты совместной разработки и условия обработки данных определяются тем же договором.
- Параметры ТЗ могут уточняться после выбора решения.