Для разработки ML-антифрод-системы в соответствии с требованиями заказчика проведём декомпозицию системы на основные функциональные компоненты. Это позволит чётко распределить задачи между командами, спланировать архитектуру и обеспечить соответствие целям по качеству, производительности, безопасности и срокам.

**🔧** Функциональная декомпозиция ML-антифрод-системы

1. Модуль приёма и предварительной обработки данных (Ingestion & Preprocessing)

Назначение: Получение транзакций в реальном времени и подготовка их к анализу.  
Функции:

* Приём входящих транзакций (в формате CSV или через API-адаптер, преобразующий CSV-поток в структурированный запрос).
* Парсинг полей транзакции (сумма, время, ID клиента, устройство, IP, геолокация и др.).
* Валидация данных (проверка на наличие обязательных полей, корректность форматов).
* Обогащение данными из внутренних источников (история клиента, средние суммы, частота операций и т.п.).
* Приведение данных к формату, пригодному для модели (нормализация, кодирование категорий).

Особенности:

* Должен поддерживать пиковую нагрузку до 400 транз./сек.
* Работает в Yandex Cloud (например, через Yandex Functions или managed-сервисы типа Yandex Data Streams).

2. Модуль извлечения признаков (Feature Engineering)

Назначение: Генерация информативных признаков для модели на основе «сырых» данных.  
Функции:

* Расчёт статических признаков (например, сумма транзакции, страна клиента).
* Расчёт агрегированных поведенческих признаков «на лету»:
  + Количество транзакций за последние 1/24 часа;
  + Отклонение суммы от среднего по клиенту;
  + Скорость смены геолокаций;
  + Признаки аномалий (например, через скользящие окна).
* Кэширование исторических признаков (в Yandex Managed Redis или YDB).
* Обработка категориальных и временных признаков (embedding, циклическое кодирование).

Особенности:

* Требуется низкая задержка (<100 мс на транзакцию).
* Поддержка онлайн- и offline-режимов (для обучения и инференса).

3. ML-модуль принятия решений (Scoring Engine)

Назначение: Классификация транзакции как «фрод» / «не фрод».  
Функции:

* Загрузка обученной модели (например, CatBoost, XGBoost или ансамбль).
* Вычисление вероятности мошенничества.
* Применение порога решения, настроенного под ограничение FPR ≤ 5%.
* Возврат бинарного решения + вероятность + (опционально) вектор признаков для объяснения.

Особенности:

* Модель должна быть интерпретируемой или поддерживать пост-хок объяснения (SHAP/LIME).
* Размещается в Yandex Cloud (например, в Yandex Serverless Containers или Yandex Compute Cloud).

4. Модуль объяснения решений (Explainability Module)

Назначение: Предоставление аналитикам и (при необходимости) клиентам объяснений блокировок.  
Функции:

* Генерация интерпретаций (например, топ-3 признака, повлиявших на решение).
* Логирование объяснений вместе с решением.
* API для запроса объяснения по ID транзакции.

Особенности:

* Обязателен для соответствия нормам прозрачности и внутренним процессам аналитиков.
* Может использовать предварительно рассчитанные SHAP-значения или lightweight-методы.

5. Модуль мониторинга и обратной связи (Monitoring & Feedback Loop)

Назначение: Контроль качества системы и сбор данных для переобучения.  
Функции:

* Логирование всех решений (разрешено/заблокировано), меток (если доступны), признаков.
* Расчёт онлайн-метрик: FPR, Recall, F0.5, средний ущерб.
* Обнаружение дрейфа данных (статистический контроль распределений признаков).
* Сбор «ground truth»: пометка транзакций как фрод/не фрод (вручную или через отложенные метки).
* Триггеры для переобучения модели (по расписанию или при падении качества).

Особенности:

* Интеграция с системами аналитики (например, Yandex Metrica, Grafana, или внутренним BI).
* Поддержка A/B-тестирования моделей.

6. Модуль управления и администрирования (Admin & Configuration)

Назначение: Настройка и управление системой без изменения кода.  
Функции:

* Настройка порога классификации (для контроля FPR).
* Управление списками доверенных/заблокированных клиентов (whitelist/blacklist).
* Конфигурация правил (например, «все транзакции > 1 млн — на ручную проверку»).
* Управление доступом и ролями (аналитик, админ, аудитор).

Особенности:

* Веб-интерфейс или API с аутентификацией (через IAM Yandex Cloud).
* Все действия логируются для аудита.

7. Инфраструктурный слой (Yandex Cloud Integration)

Назначение: Обеспечение безопасного, масштабируемого и отказоустойчивого размещения.  
Компоненты:

* Хранение данных: Yandex Object Storage (для CSV), YDB или Managed PostgreSQL (для признаков и логов).
* Вычисления: Yandex Functions / Compute Cloud / Serverless Containers.
* Сетевая безопасность: VPC, security groups, шифрование TLS.
* Аутентификация и авторизация: IAM, сервисные аккаунты.
* Мониторинг: Yandex Monitoring, Logging.

Особенности:

* Полное соответствие требованию: никаких on-premise ресурсов.
* Все данные остаются в пределах РФ (если требуется по ФЗ‑152).

**🔄** Взаимодействие компонентов (упрощённо)

1

2

3

4

5

Транзакция → [Ingestion] → [Feature Engineering] → [Scoring Engine]

↓ ↓

[Admin Rules] ← [Decision] → [Explainability] → [Monitoring & Logging]

↓

[Feedback → Retraining]

**✅** Итог

Декомпозиция выделяет 7 ключевых функциональных модулей, каждый из которых:

* решает чётко определённую задачу;
* может разрабатываться и тестироваться независимо;
* соответствует ограничениям по производительности, безопасности, интерпретируемости и срокам.

Такая структура позволяет:

* запустить MVP за 3 месяца (например, без Explainability и сложного Feature Engineering на первом этапе);
* масштабировать систему до полной версии за 6 месяцев;
* уложиться в бюджет за счёт использования managed-сервисов Yandex Cloud и open-source ML-библиотек.