Требования заказчика

В ходе детального обсуждения проекта с представителями заказчика выяснились следующие моменты:

1. Бюджетные ограничения Руководство готово выделить на реализацию данного проекта не более 10 млн рублей (не считая зарплат специалистам). Через три месяца оно хотело бы увидеть первые результаты, что позволило бы понять, стоит ли дальше развивать проект. В случае положительного решения, проект нужно завершить за полгода.

2. Требования к качеству системы Из открытых источников известно, что у ближайших конкурентов на каждую сотню проводимых их клиентами транзакций фиксируется не более двух мошеннических, приводящих к потере денежных средств. При этом общий ущерб клиентов за месяц не превышает 500 тыс. рублей. Разрабатываемая система должна выдавать результаты не хуже, иначе компания станет неконкурентоспособной.

3. Производительность системы В среднем, компания обрабатывает около 50 транзакций в секунду, однако, перед праздниками это число может достигать 400.

4. Требования к ложным срабатываниям Если система определит корректную транзакцию как мошенническую, эта транзакция будет отклонена, а пользователь будет недоволен. Опыт бизнес-аналитиков подсказывает, что если доля таких транзакций превысит 5%, то начнется отток клиентов из компании.

5. Инфраструктурные ограничения Представители компании не готовы размещать разрабатываемый модуль на собственных вычислительных ресурсах. Модуль будет размещен в облаке yandex cloud

6. Формат данных При проведении транзакции системой вся информация о ней сохраняется в виде CSV-файлов, каждая строка которых соответствует одной транзакции. Информация о транзакциях некоторого фиксированного периода помещается в отдельный файл.

7. Конфиденциальность Файлы с данными содержат всю информацию о транзакциях, включая данные клиента, который ее проводил. Данная информация является конфиденциальной, ее утечка недопустима.

На основе предоставленных требований заказчика сформулируем четкие, измеримые и достижимые цели проектируемой ML-антифрод-системы, соответствующие бизнес-контексту и ограничениям проекта.

Цели проектируемой ML-антифрод-системы

1. Обеспечение конкурентоспособного уровня защиты от мошенничества  
   Система должна обеспечивать уровень фрод-потерь не хуже рыночного бенчмарка:
   * не более 2 мошеннических транзакций на 100 обработанных;
   * общий ущерб от мошенничества не более 500 000 рублей в месяц.
2. Ограничение доли ложных срабатываний  
   Доля корректных транзакций, ошибочно классифицированных как мошеннические (false positive rate), не должна превышать 5%, чтобы избежать оттока клиентов и ухудшения пользовательского опыта.
3. Поддержка требуемой производительности в пиковые нагрузки  
   Система должна обрабатывать до 400 транзакций в секунду с задержкой принятия решения не более 200 мс на транзакцию, чтобы обеспечить бесперебойную работу в периоды высокой нагрузки (праздники, распродажи и т.п.).
4. Размещение и эксплуатация в облачной инфраструктуре  
   Весь модуль антифрода должен быть развернут и функционировать исключительно в Yandex Cloud, без использования собственных вычислительных ресурсов заказчика.
5. Обеспечение конфиденциальности и защиты персональных данных  
   Все данные, включая персональную информацию клиентов, должны обрабатываться в соответствии с требованиями законодательства (ФЗ‑152, GDPR при необходимости).  
   Реализовать:
   * шифрование данных при передаче и хранении;
   * строгий контроль доступа к данным и моделям;
   * запрет на выгрузку или копирование исходных CSV-файлов за пределы защищённой облачной среды.
6. Совместимость с существующим форматом данных  
   Система должна принимать на вход CSV-файлы с транзакциями, автоматически извлекать признаки и принимать решения без необходимости изменения формата источника данных.
7. Демонстрация измеримых результатов в течение 3 месяцев  
   К концу третьего месяца проекта должна быть представлена рабочая MVP-версия системы, способная:
   * обрабатывать реальные транзакции в тестовом или пилотном режиме;
   * продемонстрировать соответствие целям по уровню фрода и ложных срабатываний на исторических или симулированных данных;
   * обеспечить основу для принятия решения о продолжении проекта.
8. Завершение проекта в срок — в течение 6 месяцев с начала работ  
   При положительном решении после MVP-этапа система должна быть полностью развернута, протестирована и передана в эксплуатацию в течение 6 месяцев с даты старта проекта.
9. Соблюдение бюджетных ограничений  
   Общие затраты на разработку, развертывание и настройку системы (включая облачные ресурсы, лицензии, сторонние сервисы) не должны превышать 10 млн рублей.

Эти цели отражают как технические, так и бизнес-требования заказчика и могут служить основой для формирования технического задания, KPI проекта и критериев его успешности.