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

**🔍 1.** Требования к качеству (эффективность против мошенничества)

«Не более 2 мошеннических транзакций на 100» → это неверно интерпретировано!  
На самом деле: «не более 2 *успешных* мошеннических транзакций на 100 *всех* транзакций» — но это слишком много (2% = 20 000 на 1 млн транзакций).  
Скорее всего, имеется в виду:

«Не более 2 *успешных* мошеннических транзакций на 100 *тысяч* транзакций»  
(это соответствует реальной статистике: уровень мошенничества ~0.001–0.01%).

Но давайте отталкиваться от второй части требования — ущерб ≤ 500 000 ₽/мес.

**Допущения для расчёта:**

* Средний ущерб от одной успешной мошеннической транзакции: ~10 000 ₽  
  (реалистично для банковских карт: от 1 000 до 50 000 ₽).
* Тогда максимум успешных мошеннических транзакций в месяц:

10000500000​=50 транзакций

**Сколько всего транзакций в месяц?**

* Средняя нагрузка: 50 транзакций/сек
* В месяце ≈ 30 дней = 2 592 000 секунд
* Общее число транзакций в месяц:

50⋅2592000≈129.6 млн

(даже с пиковыми нагрузками — не более ~200 млн)

**Тогда допустимый** уровень пропущенного мошенничества**:**

* Допустимо 50 успешных мошеннических транзакций из, скажем, 1000 реальных попыток (предположим, что в месяц ~1000 мошеннических попыток).
* Тогда Recall (полнота) должен быть:

Recall≥1−100050​=0.95(95%)

✅ Целевой Recall ≥ 95%

**🎯 2.** Требования к ложным срабатываниям

«Если доля ложных срабатываний превысит 5%, начнётся отток клиентов».

Здесь важно понимать: 5% от чего?

* Это 5% от всех *корректных* транзакций, ошибочно заблокированных как мошеннические.
* То есть: False Positive Rate (FPR) ≤ 5%

Но в контексте несбалансированных данных удобнее использовать Precision.

Пусть:

* Общее число транзакций: 100%
* Доля мошеннических: ~0.1% (1 на 1000)
* Тогда доля легитимных: 99.9%

Если FPR = 5%, то:

* Ложных срабатываний: 5% от 99.9% ≈ 4.995% от всех транзакций
* А настоящих мошеннических, которые мы поймали (при recall=95%): 95% от 0.1% = 0.095%

Тогда Precision будет:

Precision=*TP*+*FPTP*​=0.095+4.9950.095​≈5.090.095​≈1.87%

Это очень низкая точность — почти все блокировки будут ложными!

Но бизнес говорит: «не более 5% ложных блокировок от всех *корректных* транзакций» → это FPR ≤ 5%, и это допустимо, несмотря на низкую precision.

Однако на практике банки стараются держать FPR гораздо ниже (0.1–1%), чтобы не раздражать клиентов.

**Уточнение:**

Скорее всего, бизнес имеет в виду:

«Среди всех заблокированных транзакций не более 5% должны быть ложными»  
→ Это Precision ≥ 95%

Но это противоречит требованию к ущербу (нужен высокий recall). В реальности невозможно одновременно иметь recall=95% и precision=95% при сильном дисбалансе.

**Реалистичная интерпретация:**

«Доля корректных транзакций, ошибочно заблокированных, не должна превышать 5% от всех корректных транзакций»  
→ FPR ≤ 5%

Но это слишком мягко. Вероятнее, имеется в виду:

«Не более 5% клиентов сталкиваются с ложной блокировкой в месяц»  
→ Это уже метрика на уровне пользователя, а не транзакции.

**Практическое решение:**

Будем использовать ограничение на FPR ≤ 1% (более реалистично), но формально удовлетворим требованию:

✅ False Positive Rate (FPR) ≤ 5%  
Или, что то же самое: Specificity ≥ 95%

**⚙️ 3.** Требования к производительности

* Средняя нагрузка: 50 транзакций/сек
* Пиковая нагрузка: 400 транзакций/сек
* Значит, система должна обрабатывать ≥ 400 транзакций в секунду

**Требования к задержке (latency):**

* Для онлайн-платежей: задержка < 200 мс (лучше < 100 мс)
* Это означает, что одна транзакция должна обрабатываться за ≤ 100 мс

✅ Latency ≤ 100 мс на транзакцию  
✅ Throughput ≥ 400 req/sec

**📌 Итог: Целевые метрики для ML-модели**

|  |  |  |  |
| --- | --- | --- | --- |
| Эффективность | Ущерб ≤ 500 тыс. ₽/мес | Recall (для класса «мошенничество») | ≥ 95% |
| Ложные срабатывания | Отток клиентов при >5% ложных блокировок | False Positive Rate (FPR) | ≤ 5% |
|  | (альтернатива) | Precision | По возможности ≥ 10–20% (но уступает recall в приоритете) |
| Производительность | Пиковая нагрузка 400 транз/сек | Latency | ≤ 100 мс |
|  |  | Throughput | ≥ 400 транз/сек |

💡 Главная метрика для оптимизации: Recall ≥ 95% при FPR ≤ 5%

* **🛠️ Как этого достичь?**

1. Используйте F2-score как основную метрику при подборе порога и сравнении моделей.
2. Настройте порог вероятности так, чтобы:
   * recall >= 0.95
   * fpr <= 0.05
3. Применяйте методы для несбалансированных данных:
   * class\_weight='balanced'
   * SMOTE (осторожно — может вызывать переобучение)
   * Ансамбли: BalancedRandomForest, XGBoost с scale\_pos\_weight
4. Оптимизируйте модель под latency:
   * Избегайте слишком глубоких деревьев
   * Используйте LightGBM/XGBoost (быстрые инференсы)
   * Кэшируйте feature engineering
5. Мониторинг в продакшене:
   * Отслеживайте фактический ущерб, долю ложных блокировок, latency

**📈 Пример целевой confusion matrix (на 1 млн транзакций)**

|  |  |  |
| --- | --- | --- |
| Факт: Легитим | 994 950 | 5 000(FP, FPR = 0.5%) |
| Факт: Мошенничество | 50(FN) | 950(TP) |

* Recall = 950 / (950 + 50) = 95%
* FPR = 5000 / (994950 + 5000) ≈ 0.5% (< 5% ✅)
* Precision = 950 / (950 + 5000) ≈ 16% (низко, но приемлемо при высоком recall)