**Логика работы механизма**

### 1. ****Большая сумма операции (Сумма > 100 000)****

**Логика:**

* Берём таблицу transactions, поле amount.
* Фильтруем: amount > 100000.

### 2. ****Операции в ночное время (00:00 – 06:00)****

**Логика:**

* Из поля date\_time в transactions извлекаем **время**.
* Фильтруем операции, попадающие в интервал: 00:00 <= time < 06:00.

### 3. ****Резкое изменение геолокации (изменение > 500 км)****

**Логика:**

Для каждой транзакции находим предыдущую операцию того же клиента (по client\_id и date\_time).

Определяем город:

source\_city\_id — город, откуда клиент инициировал операцию (например, его текущее местоположение).

Берем координаты городов из таблицы cities (поля latitude, longitude).

Рассчитываем расстояние между точками по Haversine формуле.

Если расстояние > 500 км и время между операциями < заданного порога (например, 12 часов) — флаг.

### 4. ****Увеличение числа операций за короткое время****

**Логика:**

Если клиент совершает **более 7 транзакций за последние 2 часа**, это считается потенциально подозрительным поведением

### 5. ****Несколько маленьких сумм вместо одной большой****

**Логика:**

* Анализируем серию операций одного клиента:
  + Несколько транзакций в течение, скажем, 30 минут–1 часа.
  + Все суммы < 10000.
  + Но в сумме превышают, например, 20000.
* Это может быть попытка обойти лимит на одну большую операцию.

### 6. ****Учет возраста клиентов (60+)****

**Логика:**

* Из clients.birth\_date определяем возраст (на основе текущей даты).
* Если возраст ≥ 60, то операции можно дополнительно проверять по всем остальным критериям.
* Возможно, применять пониженные пороги (например, меньшая сумма — уже подозрительна).

### 7. ****Переводы в рискованные страны****

**Логика:**

1. Для транзакции определяем город-получатель через destination\_city\_id.
2. Через связь cities.country\_id → countries проверяем поле blacklist:

Если blacklist = TRUE — операция подозрительна.

1. Дополнительно можно учитывать сумму (например, любые переводы в "черный список" или только крупные).

### 8. ****Категория перевода (Неизвестная)****

**Логика:**

1. Проверяем тип транзакции через связь:
   * transactions.transaction\_type\_id → transaction\_types.t\_type.
2. Флаг, если:
   * transaction\_type\_id не ссылается на существующий тип (NULL или неверный ID),
   * transaction\_types.t\_type имеет значение Unknown, Other или пустое.

**Система баллов для выявления подозрительных транзакций**

Цель: Автоматически оценивать транзакции по совокупности критериев и выявлять те, что требуют проверки или являются потенциально мошенническими.

**I. Признаки подозрительных транзакций**.

|  |  |  |
| --- | --- | --- |
| Критерий | Баллы | Описание |
| Большая сумма | 50 | Сумма транзакции > 100 000. Высокий риск отмывания средств, обход лимитов или мошенничества. |
| Операции в ночное время | 50 | Временной диапазон: 00:00–06:00. Характерно для мошеннической активности. |
| Резкое изменение геолокации | 50 | Расстояние между текущей и предыдущей транзакцией клиента > 500 км за короткий промежуток времени (например, 1 час). Указывает на компрометацию данных. |
| Увеличение числа операций | 30 | Резкий всплеск активности (например, количество операций за сутки значительно превышает среднее за месяц). Может указывать на попытку быстро вывести средства. |
| Несколько маленьких сумм вместо одной большой | 30 | Серия мелких переводов (например, по 1–5 тыс.) в течение короткого времени, которые в сумме превышают пороговую сумму. Подозрение на дробление платежей. |
| Категория перевода: "Неизвестная" | 30 | Тип транзакции не определён, отсутствует в справочнике, не имеет чёткого назначения. Может маскировать запрещённую деятельность. |
| Переводы в рискованные страны | 40 | Получатель находится в юрисдикции, включённой в чёрный список (например, FATF, OFAC и др.). Независимо от суммы или времени — это критический флаг. |

**II. Модификаторы риска (усиливающие факторы)**

|  |  |  |
| --- | --- | --- |
| Критерий | Баллы / Поведение | Описание |
| Клиент в возрасте 60+ | +20 / или +10% ко всем баллам | Люди пожилого возраста чаще становятся жертвами мошенников. При наличии других признаков — повышает риск. |

**Правила принятия решения**

|  |  |
| --- | --- |
| Обычная | Сумма баллов < 50, и нет приоритетных признаков. |
| Требует проверки | Сумма баллов от 50 до 79 |
| Подозрительная | Сумма баллов ≥ 80 |
| Красный флаг | всегда флаг. |

**Примеры расчёта баллов**

Пример 1:

Сумма = 150 000 → +50

Время = 01:30 → +50

Возраст клиента = 67 лет → +20

**Итог**: Подозрительная (баллы = 120+)

Пример 2:

5 операций по 25 000 в течение 30 минут → +30

Категория перевода: Неизвестно → +30

Возраст клиента: 72 года → +20

**Итог**: 80 баллов → Подозрительная

Пример 3:

Перевод на 20 000

В 10:00 утра

Получатель в оффшорной зоне → +40

**Итог**: Требует проверки

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Критерии (сокр.) | Баллы (П+В) | Возраст 60+ | Общие баллы | Статус | Комментарий |
| 1 | П: Сумма + В: Частота | 50 + 30 | — | 80 | Подозрительная | Большая сумма (приоритет) + частота. Порог превышен. |
| 2 | П: Гео + В: Категория | 50 + 30 | — | 80 | Подозрительная | Приоритетный критерий (гео) автоматически вызывает подозрение. |
| 3 | В: Частота + Категория | 30 + 30 | — | 60 | Требует проверки | Без приоритетных критериев — стандартная проверка. |
| 4 | П: Время + П: Сумма | 50 + 50 | — | 100 | Подозрительная | Два приоритетных критерия — немедленный флаг. |
| 5 | В: Частота + Малые суммы + Категория | 30 + 30 + 30 | — | 90 | Подозрительная | Накопленные баллы превышают порог (80). |
| 6 | П: Гео + В: Частота + Категория | 50 + 30 + 30 | — | 110 | Подозрительная | Приоритетный критерий (гео) + усиление вторичными. |
| 7 | В: Частота + Малые суммы | 30 + 30 | ✅ (+20) | 80 | Подозрительная | Возрастной модификатор усилил риск до критического уровня. |
| 8 | П: Время + В: Категория + Частота | 50 + 30 + 30 | — | 110 | Подозрительная | Приоритетный критерий (время) + дополнительные факторы. |
| 9 | В: Малые суммы + Категория + Страна | 30 + 30 + 40 | — | 100 | Подозрительная | Рискованная страна (критический флаг) усилил подозрение. |
| 10 | В: Частота + Категория | 30 + 30 | ✅ (+20) | 80 | Подозрительная | Возрастной модификатор довел баллы до порога. |
| 11 | П: Гео + П: Время + В: Малые суммы | 50 + 50 + 30 | — | 130 | Подозрительная | Два приоритетных критерия + дополнительный риск. Автоматический флаг. |
| 12 | П: Время + В: Категория + Страна | 50 + 30 + 40 | ✅ (+20) | 140 | Подозрительная | Высокий риск (время + страна) + возрастной модификатор. Требует блокировки. |

**П** – Приоритетный критерий (сразу делает транзакцию подозрительной)

**В** – Вторичный критерий (баллы суммируются)

**М** – Модификатор риска (возраст 60+)

**Расчет итогового балла и статус**

**if** has\_priority\_flag:

status = "Подозрительная"

**elif** total\_score >= **80**:

status = "Подозрительная"

**elif** **50** <= total\_score < **80**:

status = "Требует проверки"

**else**:

status = "Обычная"

**Видение в Python**

1. **Большая сумма операции**

transactions[transactions['amount'] > 100000]

**2. Операции в ночное время**

transactions[transactions['time'].between(time(0, 0), time(6, 0))]

3. **Резкое изменение геолокации**

1. Группируем по client\_id + сортируем по времени.
2. Для каждой транзакции:
   * Берем предыдущую операцию клиента.
   * Считаем расстояние (Haversine) между городами.
   * Фильтруем: distance > 500 и time\_diff < 3h.

4. **Резкий рост числа операций**

lient\_groups = transactions.groupby('client\_id').rolling('2H', on='date\_time').count()  
client\_groups[client\_groups > 7]

5. **Несколько маленьких сумм вместо одной большой**

1. Группируем по клиенту + окну 1 час.
2. Фильтруем группы, где:
3. Каждая операция <10K, но сумма >20K.

6. **Категория перевода — неизвестная**

clients[ (current\_year - clients['birth\_date'].dt.year) >= 60 ]

7. **Перевод в рискованные страны**

transactions.merge(cities).merge(countries)[countries['blacklist'] == True]

**8. Возраст клиента ≥ 60 лет**

transactions[transactions['transaction\_type\_id'].isna() | transactions['t\_type'].isin(['Unknown', ''])]

+ Нужно сделать так, чтобы данная категория везде добавляла 20 к риску