

Наименование задачи (проекта)

Антифрод-защита OTP-верификации номера телефона: снижение фрод-отправок SMS при сохранении доступности сервиса для реальных пользователей

Цель и описание задачи (проекта)

Цель - спроектировать систему верификации и аутентификации клиента по номеру телефона, которая:

- выявляет и блокирует автоматические запросы OTP (боты, перебор номеров, SMS pumping);
- не блокирует реальных пользователей из любых стран (Казахстан, Центральная Азия, Россия, другие);
- минимизирует затраты на SMS за счёт снижения доли мусорных отправок.

Участник проектирует целевой workflow входа/регистрации и антифрод-контур: последовательность шагов, каналы верификации (SMS OTP, flash-call, мессенджер-OTP, silent network auth и др.), скоринг рисков (risk-engine на поведенческих, device и сетевых сигналах), политику блокировок и деградации, метрики эффективности. Существующий workflow может быть перепроектирован полностью.

Результат - проектный документ (дизайн-решение): архитектура, workflow, логика антифрода, обоснование trade-offs. Код не требуется.

Описание проблемы

Ticketon использует номер телефона для верификации и аутентификации: клиент вводит номер, сервис отправляет SMS с OTP, клиент вводит код в форму. Схема рабочая, но ею злоупотребляют.

Конкуренты и злоумышленники через ботнет-сеть массово отправляют форму и инициируют SMS на произвольные номера. Цель атаки - искусственно раздуть счёт за SMS без реального использования сервиса.

Текущее состояние:

- CloudFlare Captcha установлена, но боты её обходят;
- около 30% OTP-отправок - фрод;
- конверсия отправленных OTP в подтверждённые - 60%;
- ложные блокировки реальных пользователей не измеряются - метрики нет;
- фильтрация по коду страны невозможна: аудитория глобальная, малые страны (например, Вьетнам) дают легитимный трафик.

Экономический эффект атаки: ~18 000 фрод-отправок в месяц, ~126 000 KZT прямых потерь ежемесячно, плюс риск недоступности сервиса для реальных клиентов при агрессивных блокировках.

T3

Спроектировать антифрод-контур верификации/аутентификации по номеру телефона:

1. Целевой workflow входа и регистрации: шаги, каналы верификации, порядок их применения, fallback-сценарии.
2. Risk-оценку запроса до отправки SMS: сигналы (поведенческие, device fingerprint, IP/сеть, история номера, частота), скоринг, пороги, действия по уровням риска (пропустить, усилить проверку, отказать).
3. Политику rate-limit и блокировок, исключаящую массовые ложные срабатывания на реальных пользователях.
4. Метрики: доля фрод-отправок, конверсия OTP, доля ложных блокировок, стоимость верификации на пользователя.
5. Если решение меняет канал аутентификации (например, SMS на email или мессенджер) - обязателен план миграции существующей базы клиентов с оценкой трудозатрат в днях.

Формат сдачи - проектный документ. Развёрнутое T3 приложено отдельным файлом (см. ниже).