Как оценить влияние DS-метрик на итоговые бизнес-результаты проекта

Павел Филонов

План

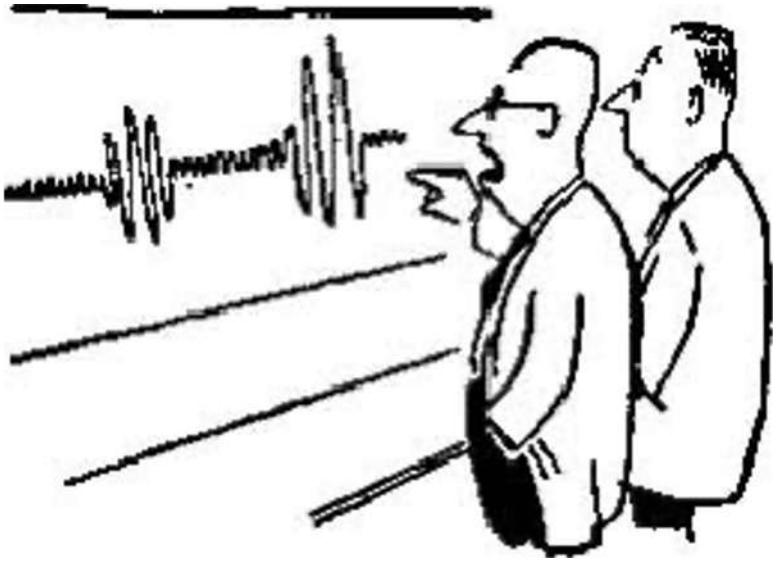
- Заходят в бар DS и бизнес аналитик
- Пирамида ~~шампанского~~ метрик
- 3 шота
  - ложь, наглая ложь и статистика
  - давай сделаем это по быстрому
  - учат в школе, учат в школе, учат в школе
- на посошок

Ваш бармен на сегодня

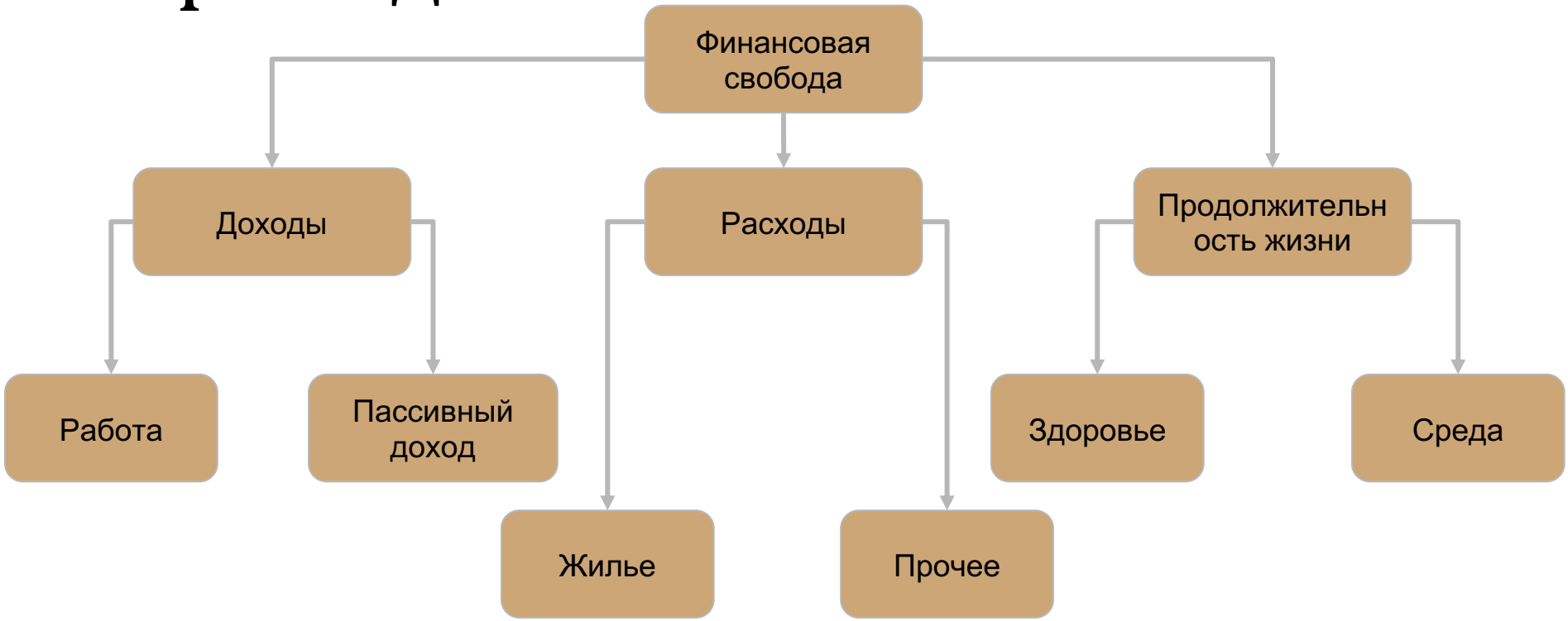
- преподаватель
- разработчик (C++, Python)
  - Max Patrol SIEM
  - Kaspersky MLAD, MDR
- датасаентист
- независимый консультант

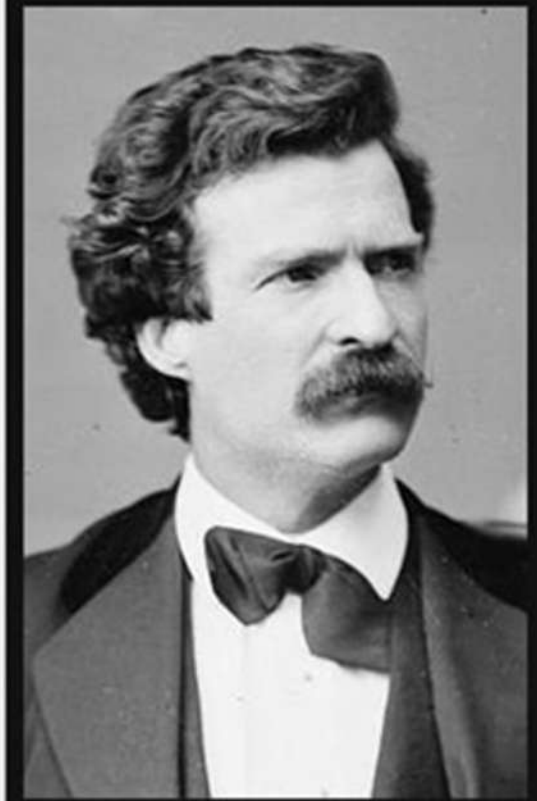
Заходят в бар DS и бизнес аналитик

- Профессор, мы из эксперимента получили такой график, но не можем его объяснить.
- Так это же очень просто!
- Профессор, но Вы держите его неправильно, нужно перевернуть.
- Так это еще проще!



Пирамида


Финансовая свобода
Доходы
Расходы
Продолжительность жизни
Работа
Пассивный доход
Жилье
Прочее
Здоровье
Среда

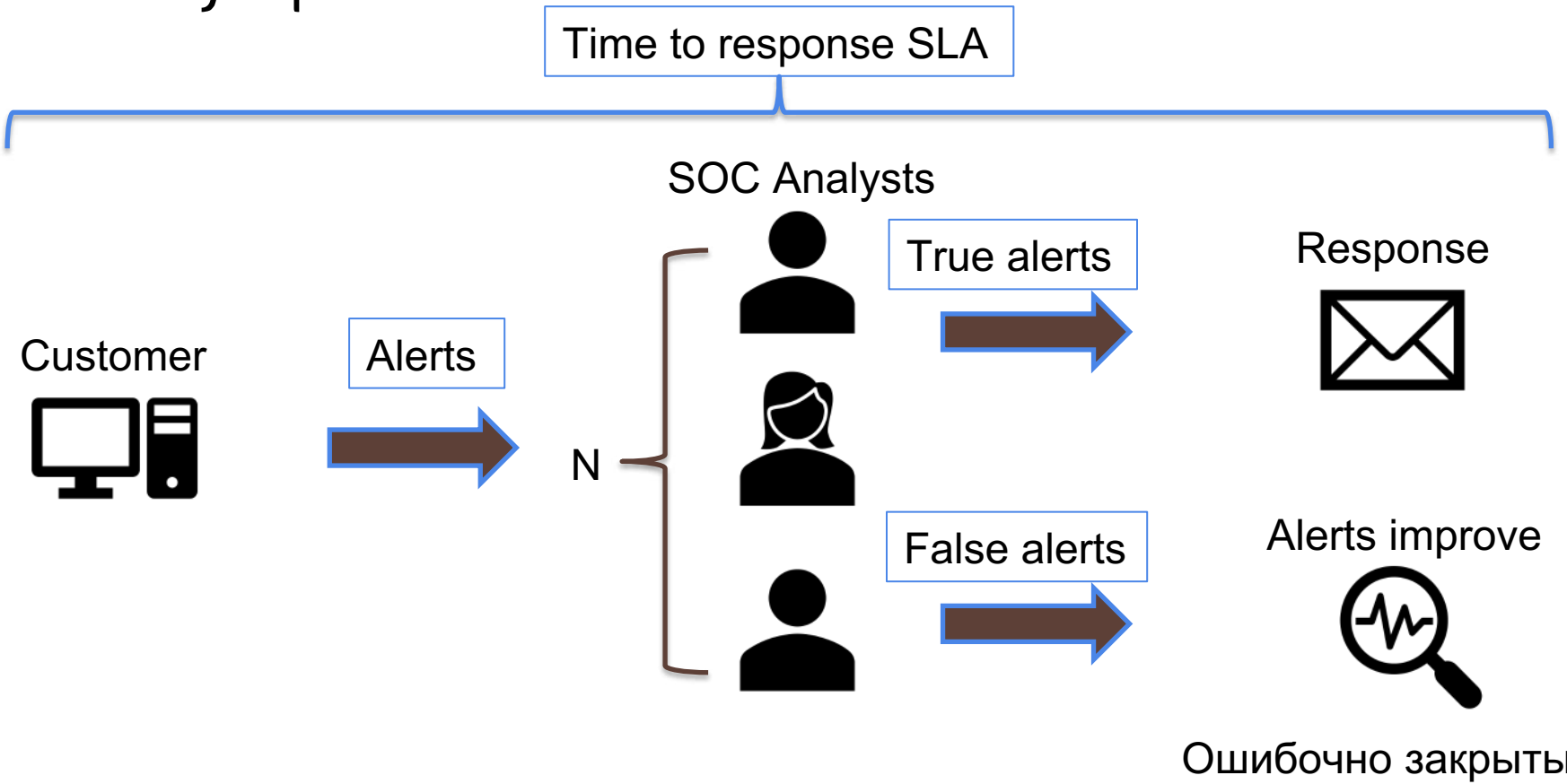


Существуют три вида лжи: ложь, наглая ложь и статистика.

(Марк Твен)

tsitaty.com

Security Operation Center



Метрики SOC

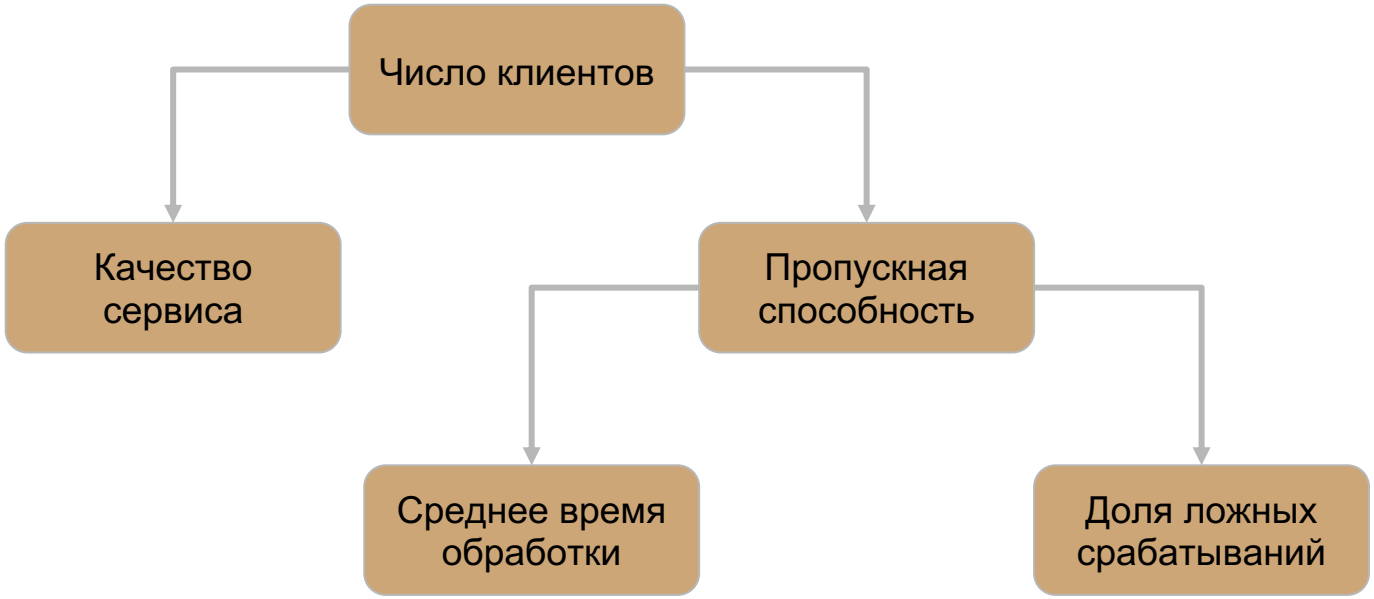
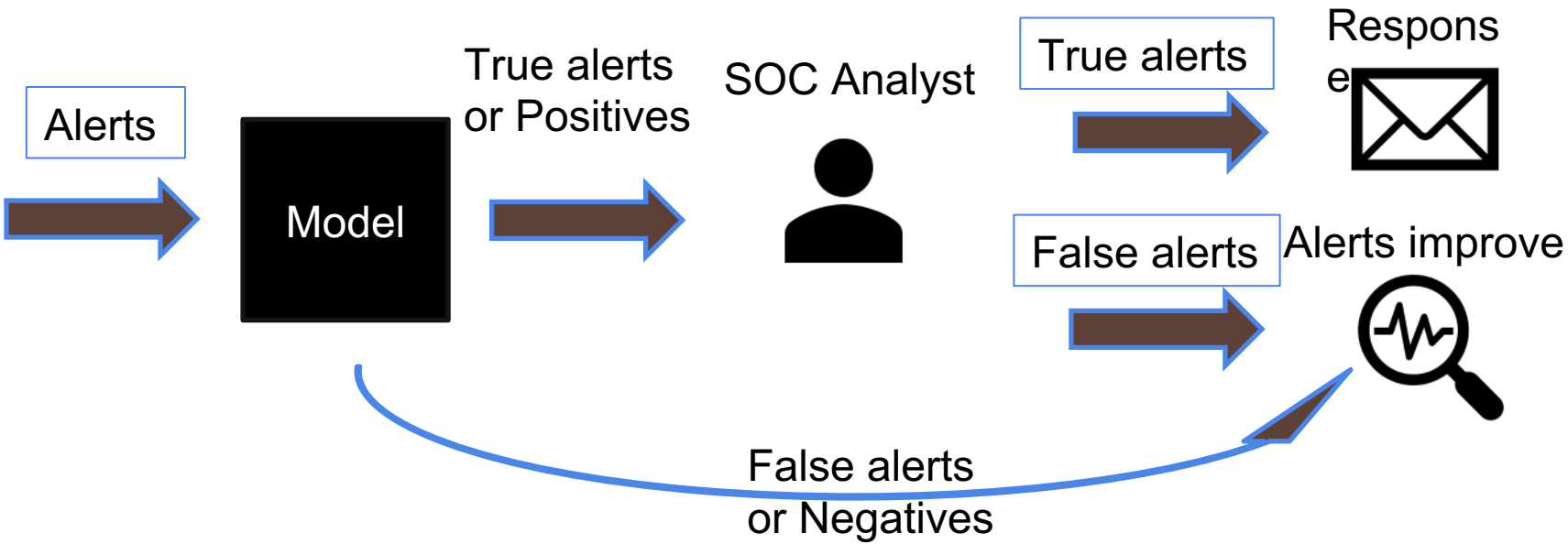
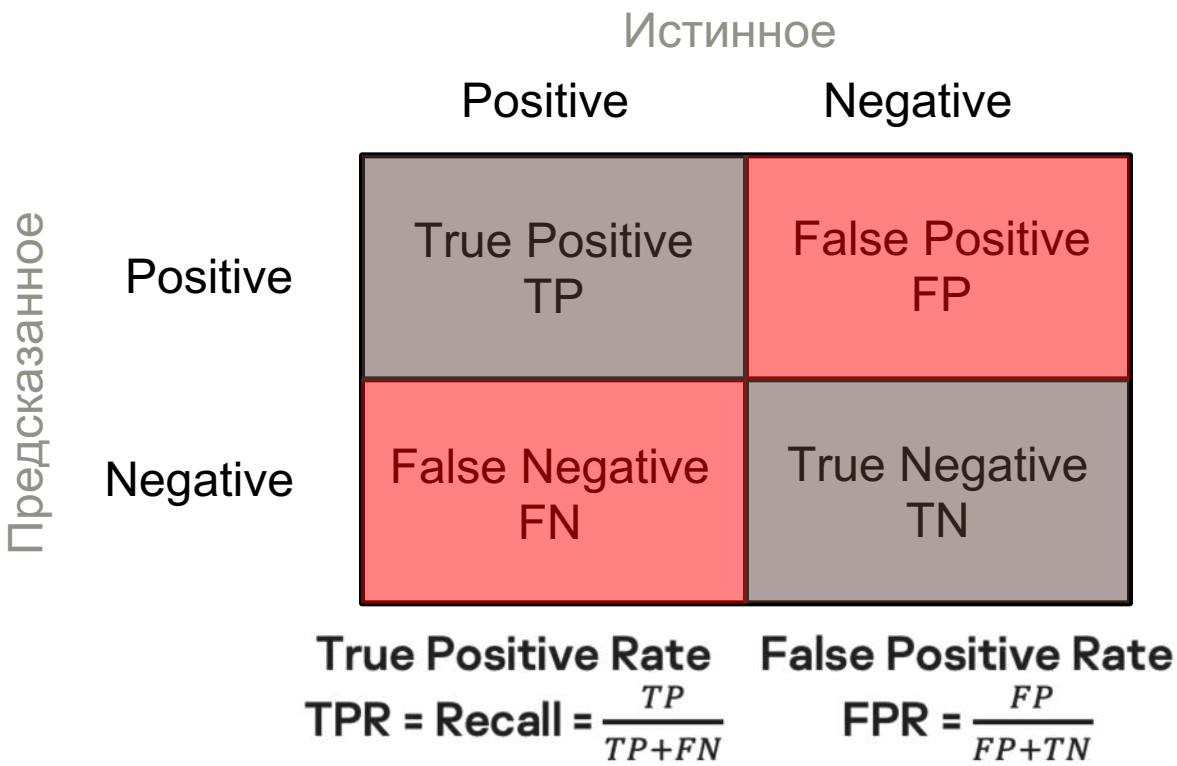

Число клиентов
Качество сервиса
Пропускная способность
Среднее время обработки
Доля ложных срабатываний

Схема реализации



Матрица ошибок

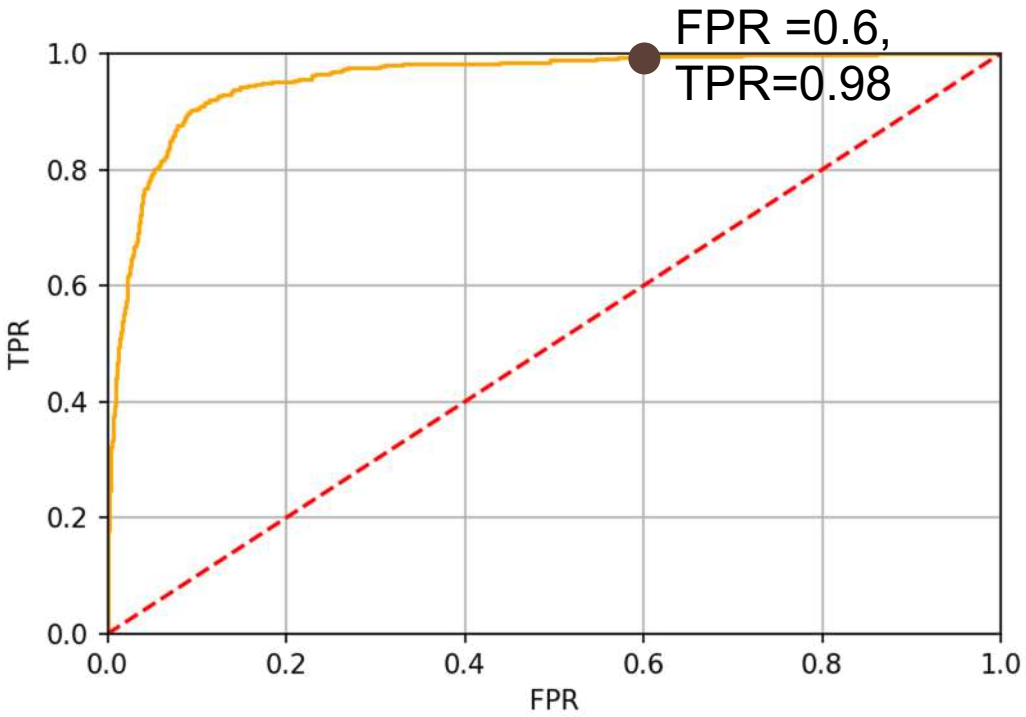


FPR модели 0.6:

60% всех негативных примеров будут распознаны некорректно

Вывод – можно автоматически отфильтровать 40% всех ложных оповещений, что повысит **пропускную способность**

ROC кривая

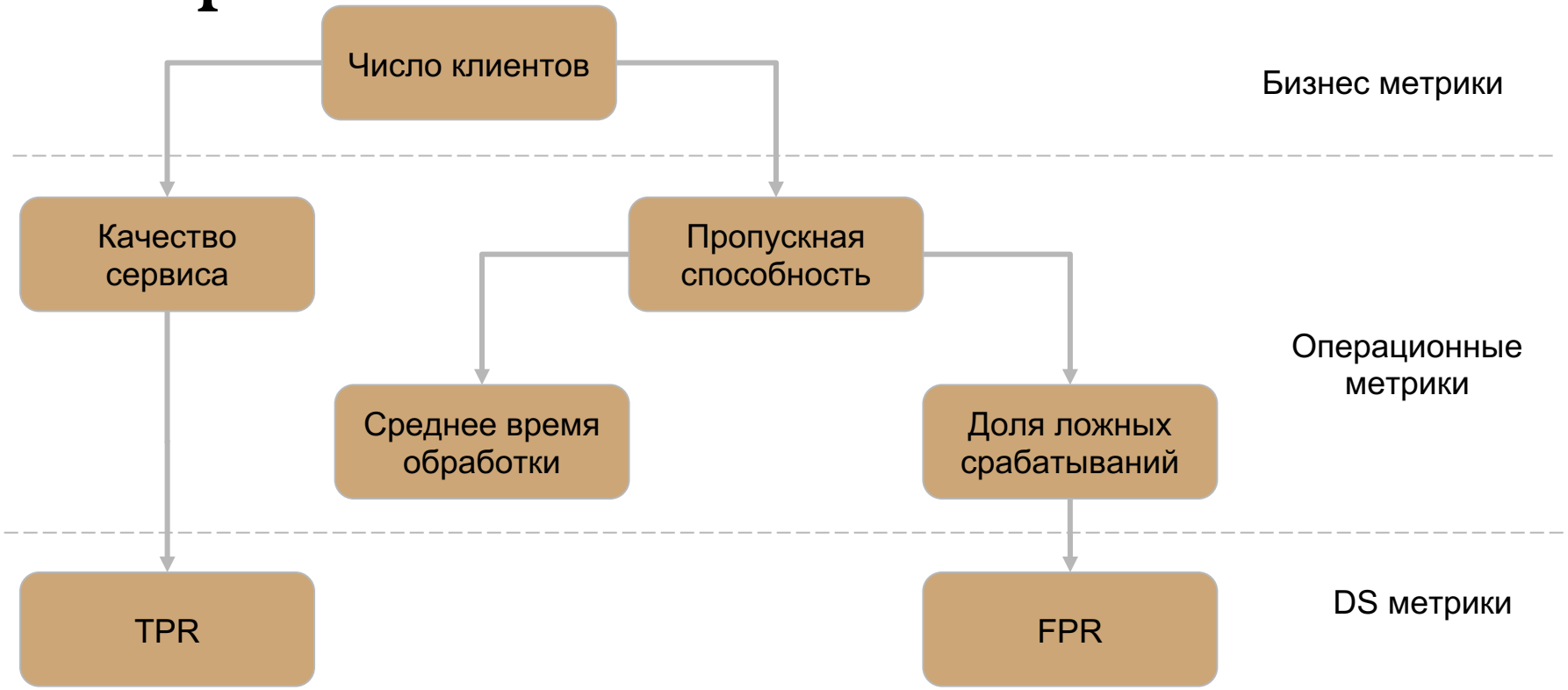


Модель может автоматически отфильтровать **40%** ложных оповещений.

При этом доля ошибочно закрытых составит **2%**

Эксперимент показал, что пропускная способность аналитика растет с уменьшение FPR.

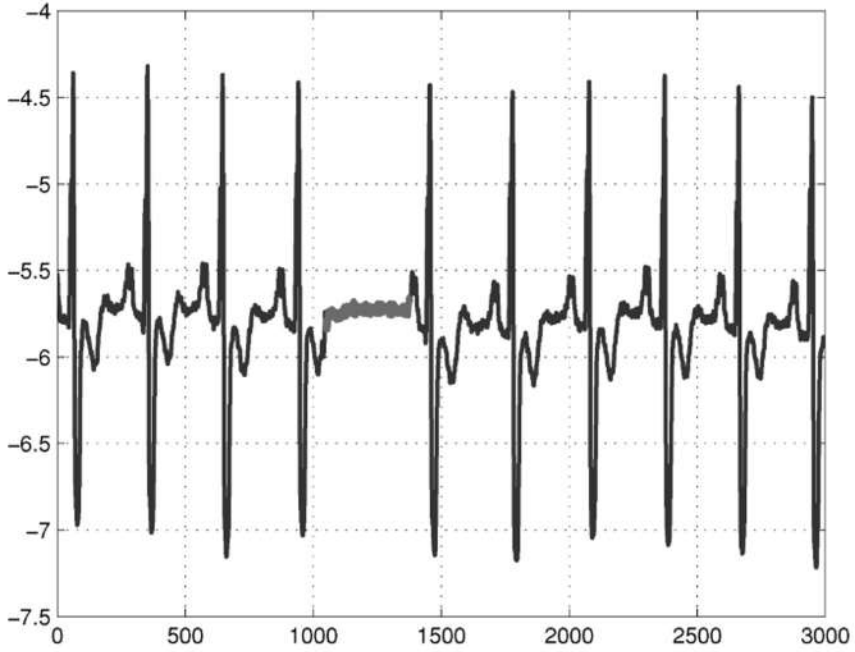
Метрики SOC


Число клиентов
Качество сервиса
Пропускная способность
Среднее время обработки
Доля ложных срабатываний
TPR
FPR
Бизнес метрики
Операционные метрики
DS метрики

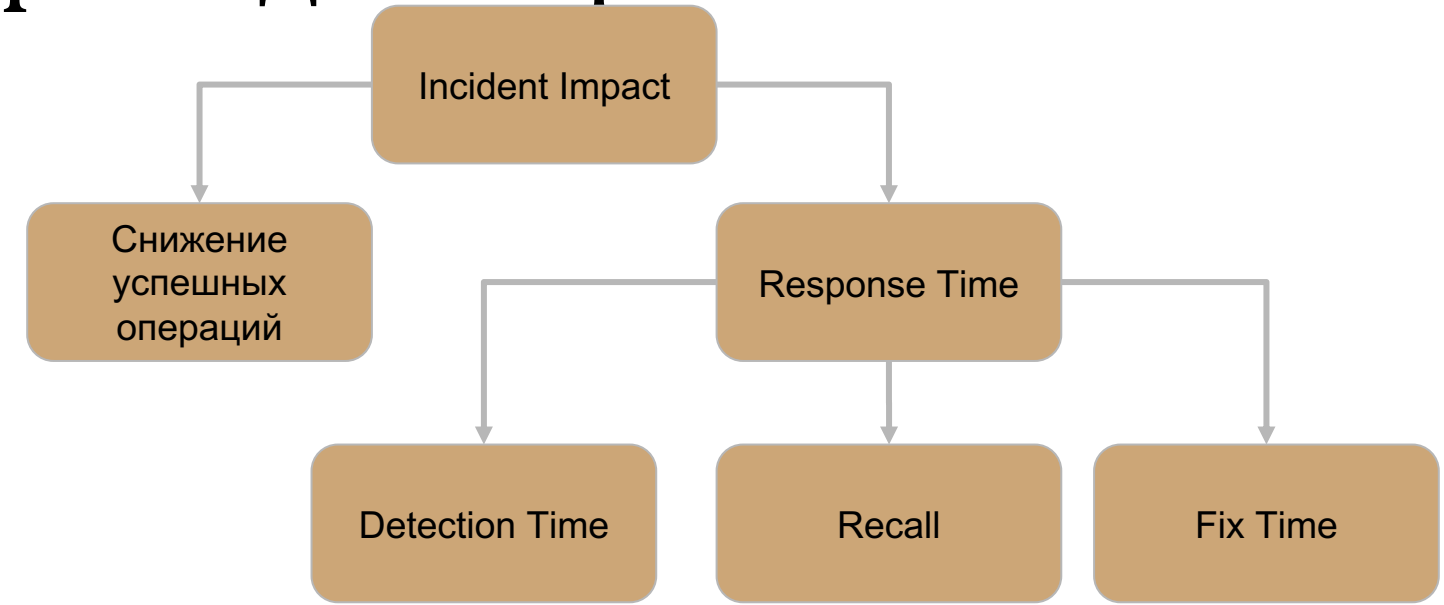

TOUCHSTONE PICTURES AND JERRY BRUCKHEIMER PRESENTS
GONE IN 60 SECONDS
NICOLAS CAGE "GONE IN 60 SECONDS" ANGELINA JOLIE GIOVANNI RIBISI DELROY LINDO WILL PATTON CHRISTOPHER ECCLESTON CHI McBRIDE AND ROBERT DUVALL
MUSIC BY TREVOR RABIN EDITED BY TOM MOLOOSIN CHRIS LEBENZON DIRECTOR OF PHOTOGRAPHY PAUL CAMERON SCREENPLAY BY SCOTT ROSENBERG EXECUTIVE PRODUCERS JONATHAN HENSLEIGH CHAD OMAN BARRY WALDMAN
PRODUCED BY JERRY BRUCKHEIMER MIKE STENSON DIRECTED BY DOMINIC SENA
TOUCHSTONE PICTURES

Мониторинг платежной системы

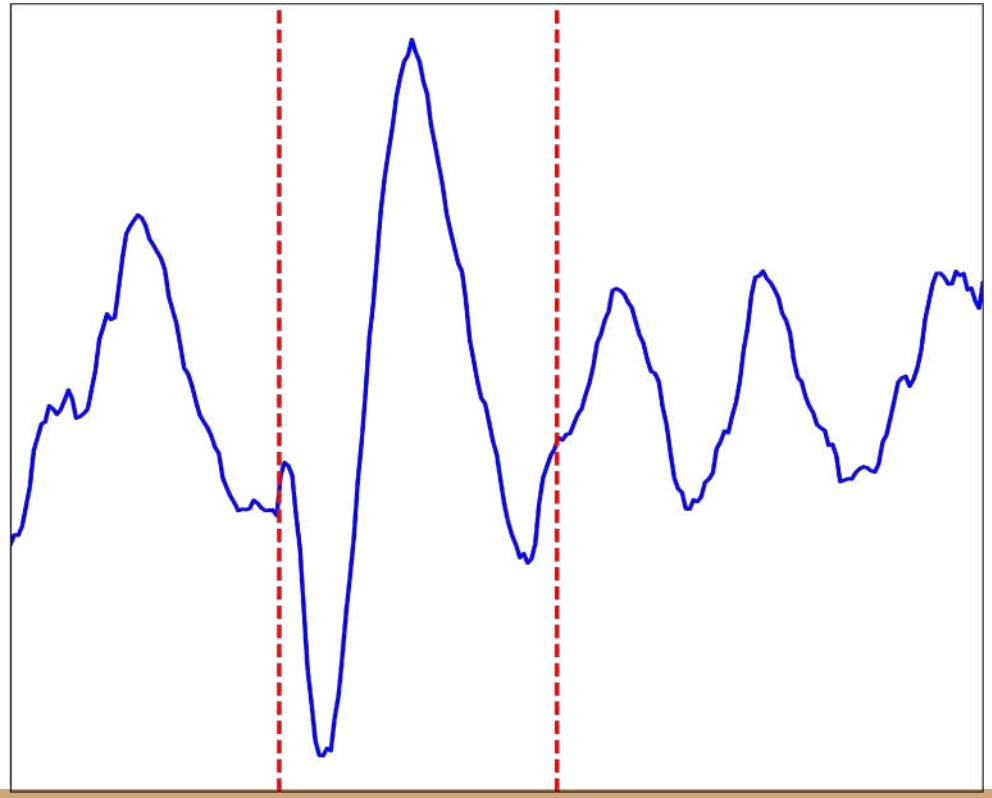
- объемы входящих транзакции
- успешные/неуспешные платежи
- тысячи графиков
- частые инциденты
- большое время реагирования



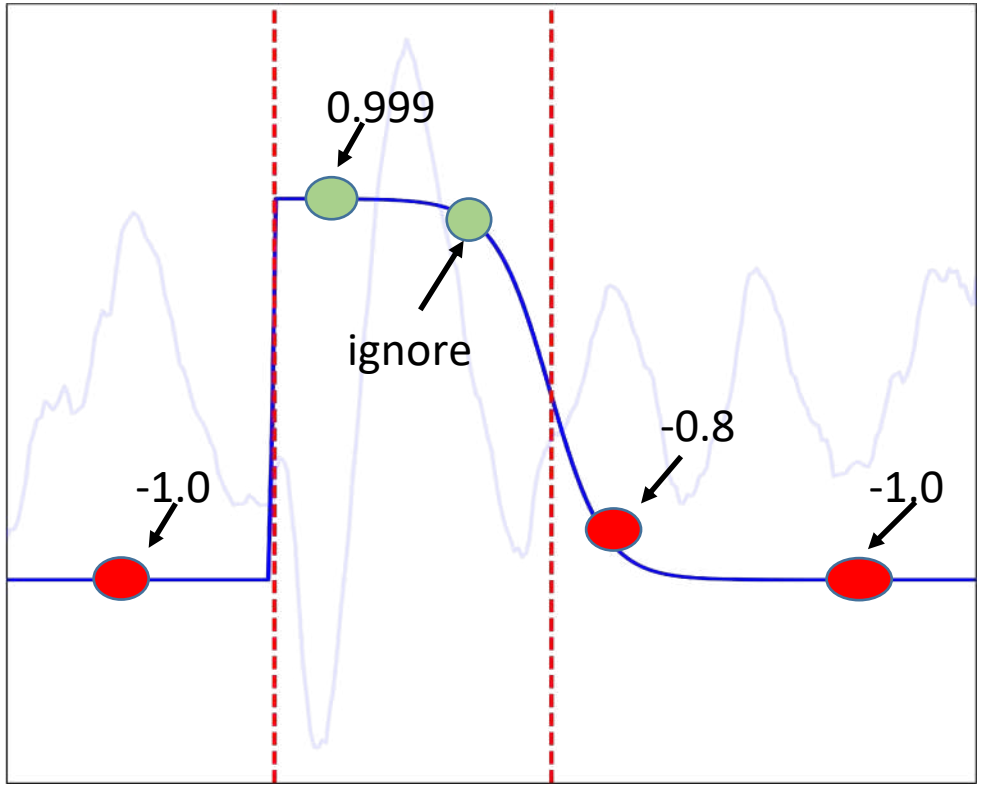
Пирамида метрик



Окно аномального поведения

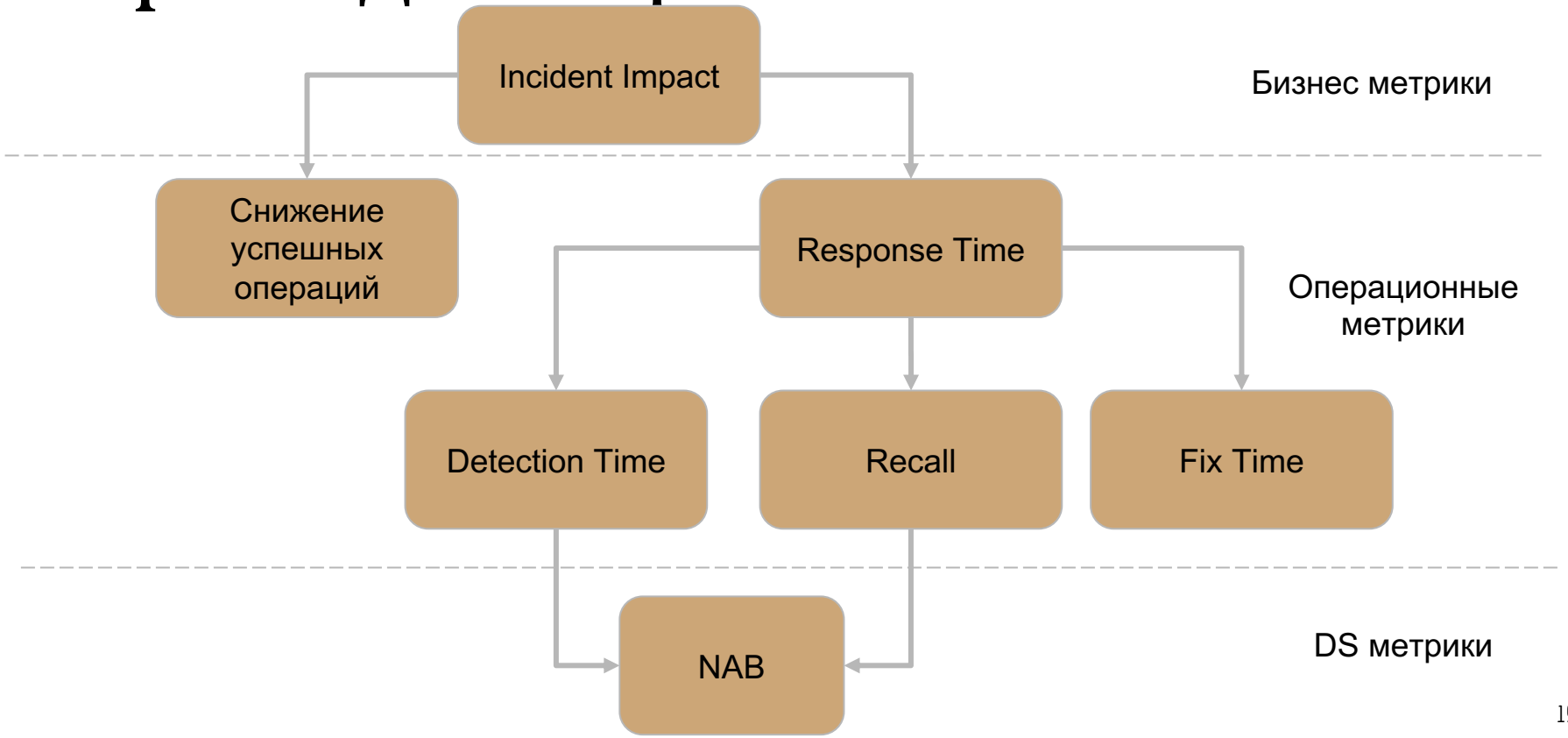


Numenta Anomaly Benchmark Score



- награждаем за раннее обнаружение
- штрафуем за позднее обнаружение
- штрафуем за необнаружение
- штрафуем за ложное срабатывание

Пирамида метрик




I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL OVER THE WALLS
I MUST NOT WRITE ALL
MATT GROENING

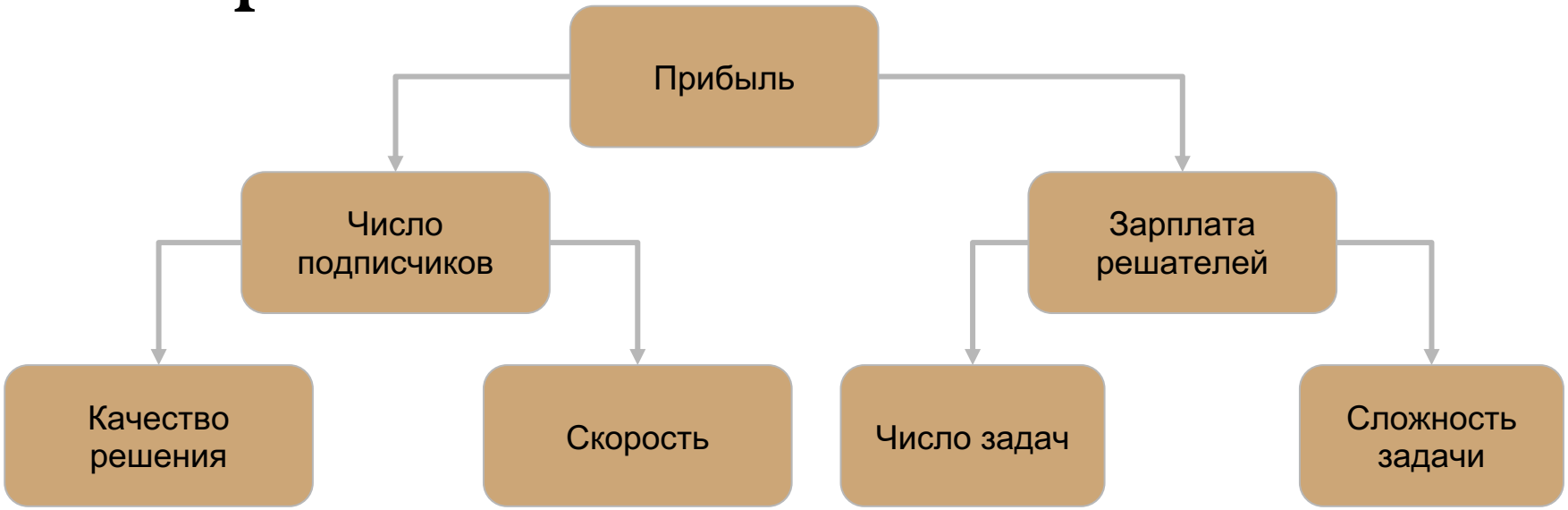
Реши за меня пример

Школьник

Решатель

Решение

Метрики


Прибыль
Число подписчиков
Зарплата решателей
Качество решения
Скорость
Число задач
Сложность задачи

Как автоматизировать

- распознавание текста, формул и графиков
- ChatGPT (тогда не было)
- готовые решатели
  - разбиение на подзадачи
  - классификация задач
  - формулировка в стандартном виде
- поиск похожих задач с решениями

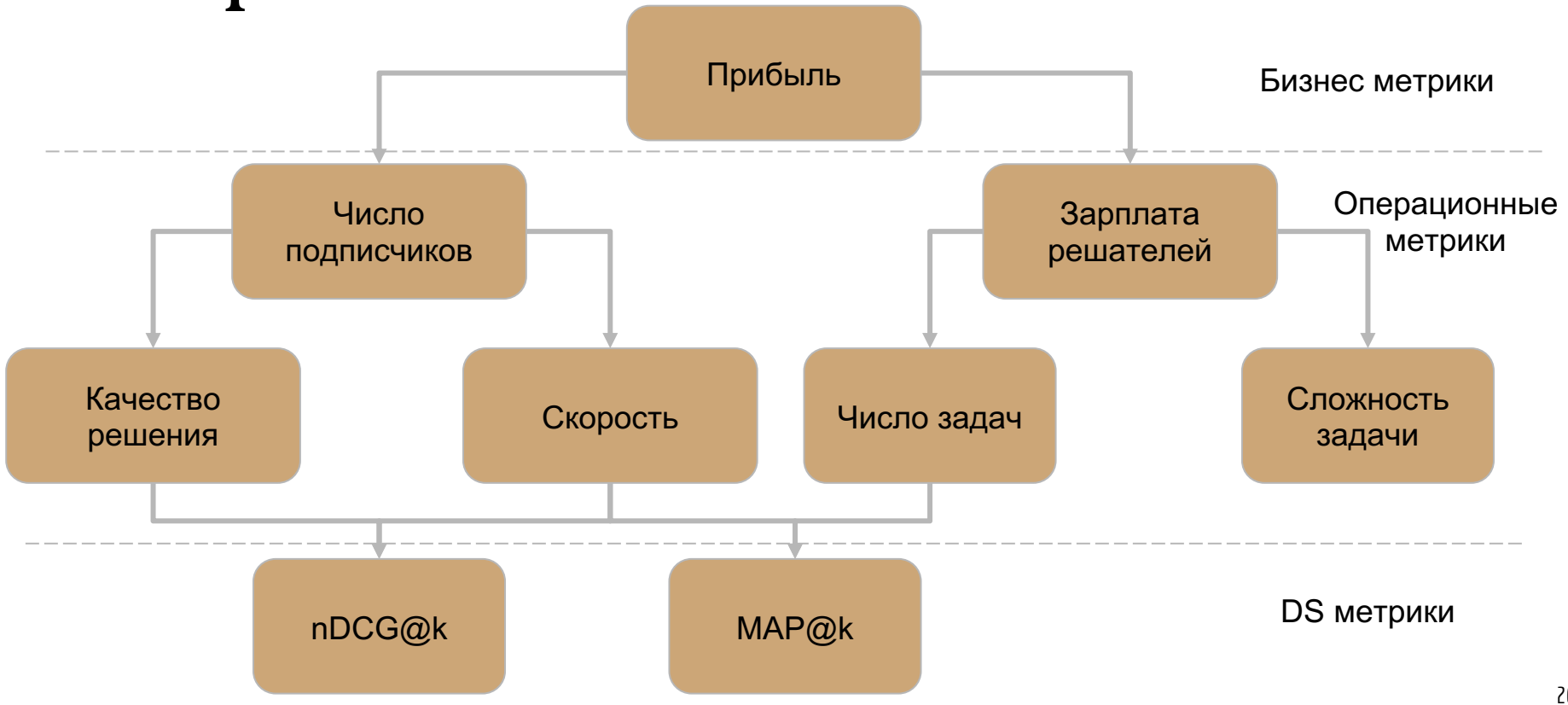
Поиск

- задач много
- точного совпадения текстов может не быть
- не получится выдать в ответ 1000 результатов
- если результат поиска не удовлетворил, то отправляем на сложные алгоритмы или людей

Метрики ранжирования

- MAP@k - подходит для бинарных ответов
- nDCG@k - может учитывать вес ответа

Метрики


Прибыль
Бизнес метрики
Число подписчиков
Зарплата решателей
Операционные метрики
Качество решения
Скорость
Число задач
Сложность задачи
nDCG@k
MAP@k
DS метрики


НА ПОСОШОК
1795

На посошок

- найдите общий язык с DS
- свяжите DS и бизнес метрики через proxy
- убедитесь, что они коррелируют
- измеряйте DS метрики чаще
- доверяй, но проверяй

Спасибо за внимание!