Опять двадцать пять, или Как не допустить повторения инцидента

Кирилл Борисов, VK

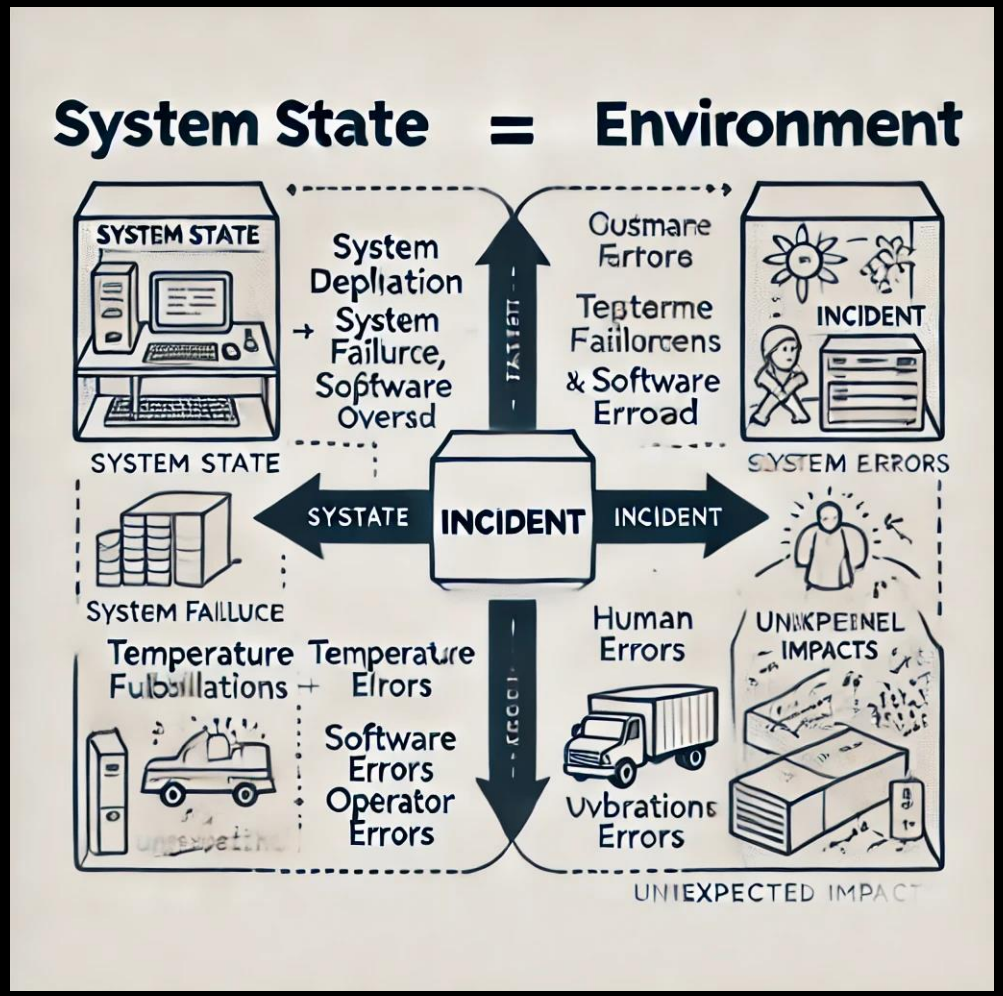
$whoami

- В IT более 13 лет
- Строил DevOps-процессы и инфраструктуру в больших проектах
- SRE в VK
- Спикер Slurm, DevOps, Devoops, Highload

Инцидент

Незапланированное прерывание ИТ услуги или ухудшение качества ее предоставления…

Состояние системы + Среда = Инцидент



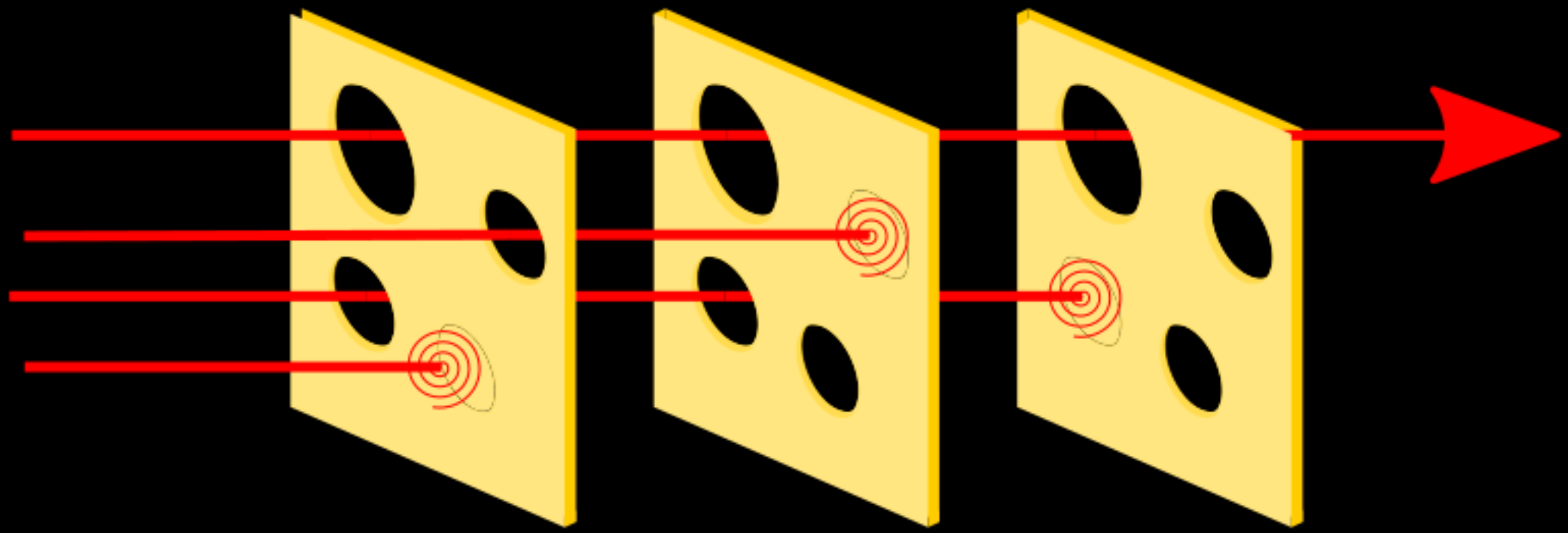
Состояние системы

- Технические элементы
- Организационные аспекты
- Человеческий фактор

Среда

- Физические условия
- Внешние воздействия
- Организационные и социальные факторы

Swiss Cheese Model



Swiss Cheese Model

- Защита и барьеры
- Уязвимости
- Выравнивание

Недостаточное извлечение пользы

- Предвзятость ретроспективного подхода
- «Соблазнение» первопричиной
- Обвинение человека

Предвзятость ретроспективного подхода

- Иллюзия предсказуемости
- Преувеличение роли очевидных факторов

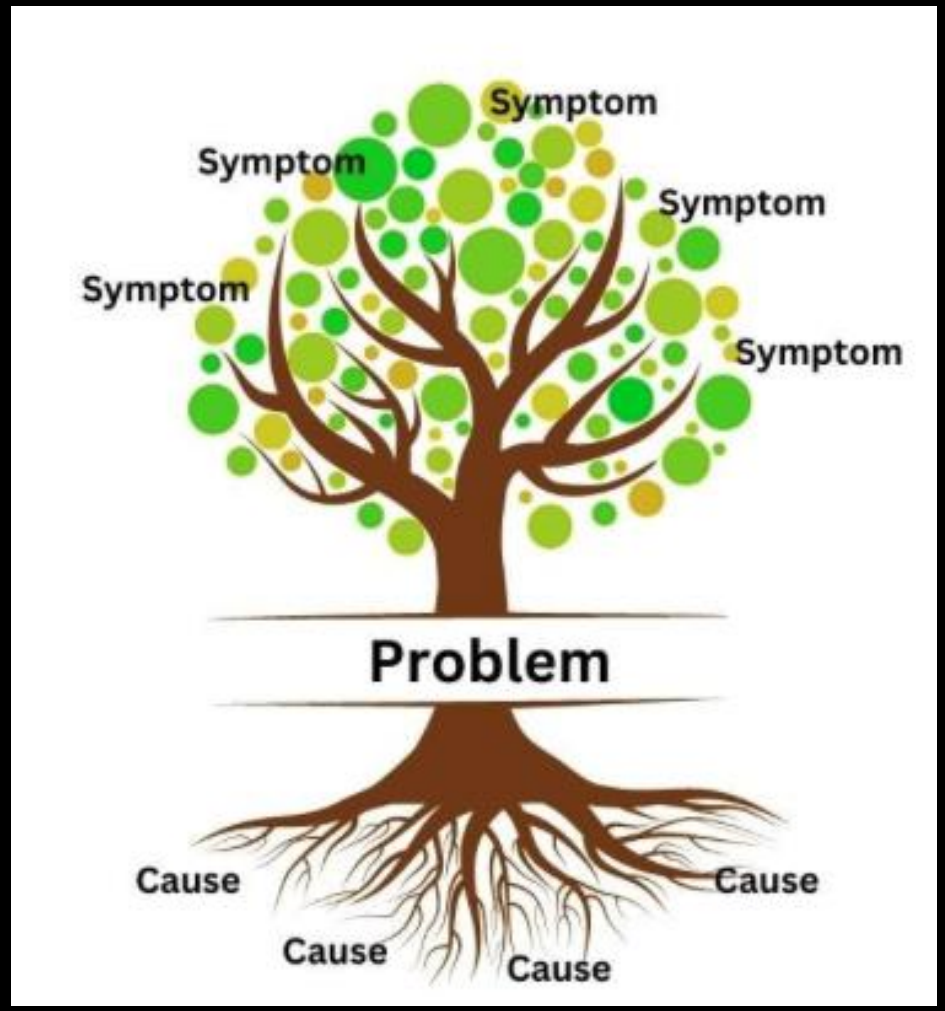
«Соблазнение» первопричиной

- Фокусировка на одной причине
- Упрощение связей

Обвинение человека

- Сложность систем
- Системные и организационные факторы
- Культура открытости

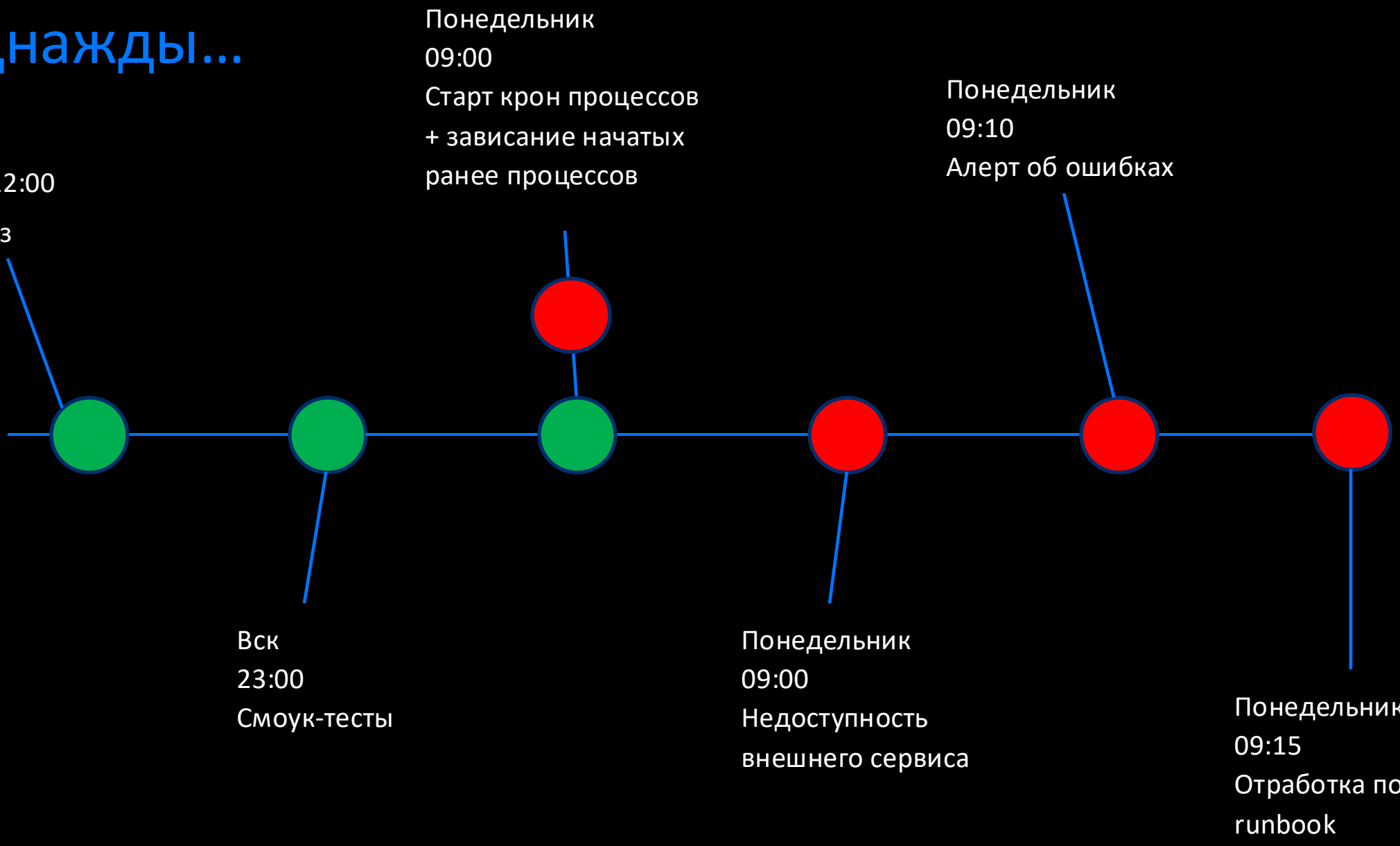
RCA


Symptom
Symptom
Symptom
Symptom
Symptom
Problem
Cause
Cause
Cause
Cause

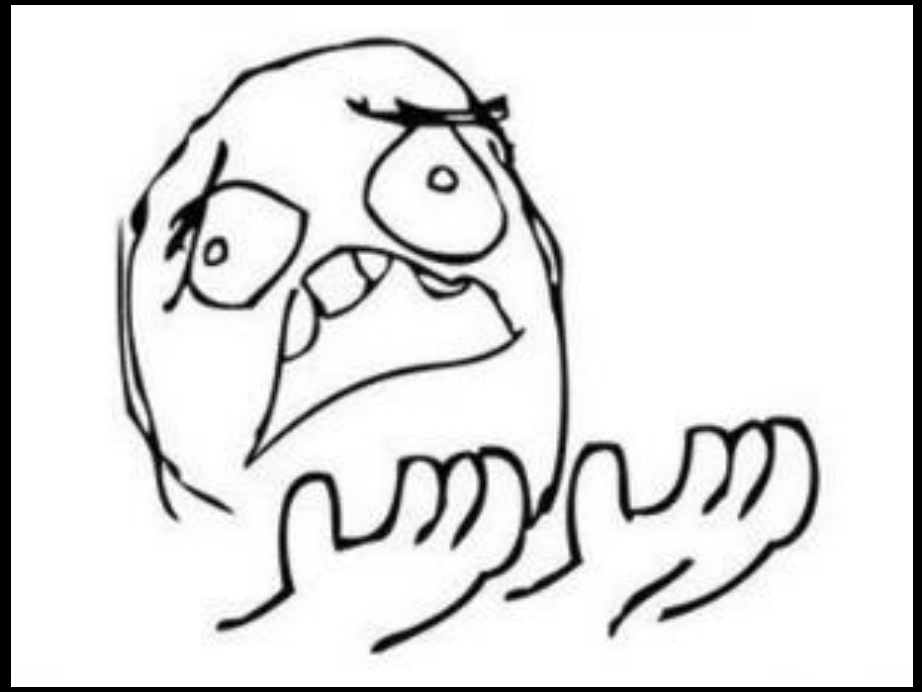
RCA

- 5 WHYS
- Fishbone Diagram
- FMEA

Однажды...


Вск 22:00
Релиз
Вск
23:00
Смоук-тесты
Понедельник
09:00
Старт крон процессов
+ зависание начатых
ранее процессов
Понедельник
09:00
Недоступность
внешнего сервиса
Понедельник
09:10
Алерт об ошибках
Понедельник
09:15
Отработка по
runbook

5 WHYS



WHY 1

Почему произошло дублирование начислений на счетах клиентов?

WHY 2

Почему процессы были принудительно продвинуты по новой версии схемы?

WHY 3

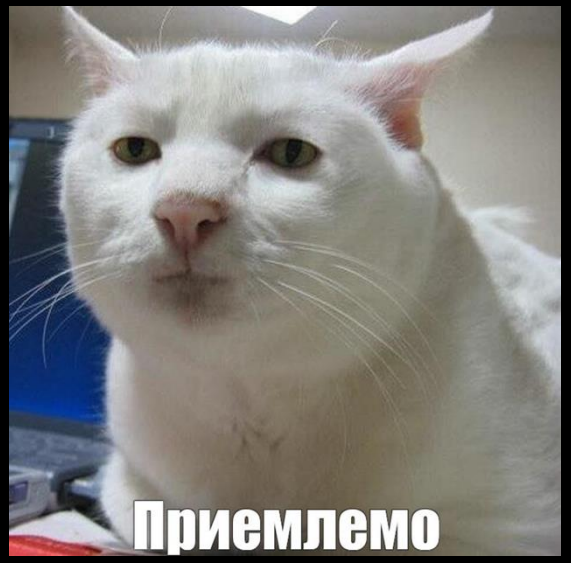
Почему новая версия не поддерживала корректное выполнение незавершенных процессов?

WHY 4

Почему архитектура не предусматривала обработку переходящих процессов?

WHY 5

Почему требования к переходу версий были проработаны недостаточно?



Root Cause

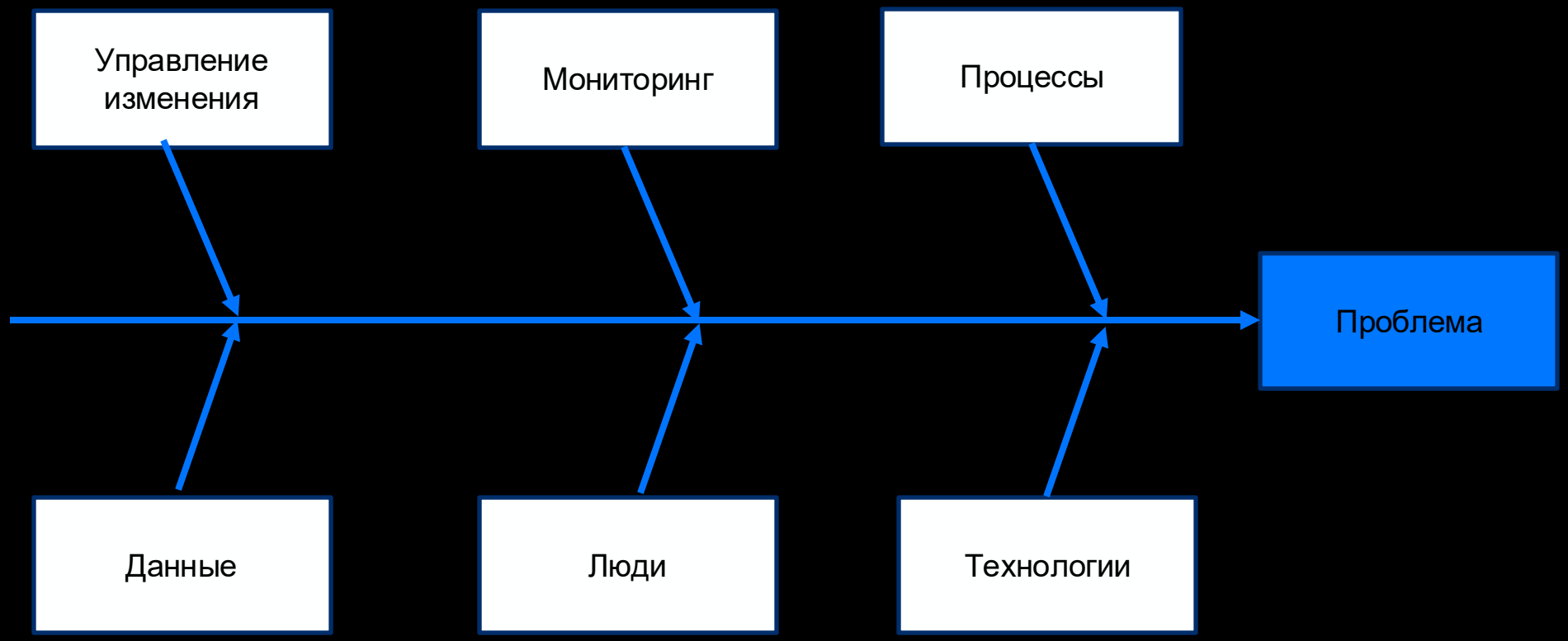
- Непроработанная архитектура
- Отсутствие требований

Границы применимости

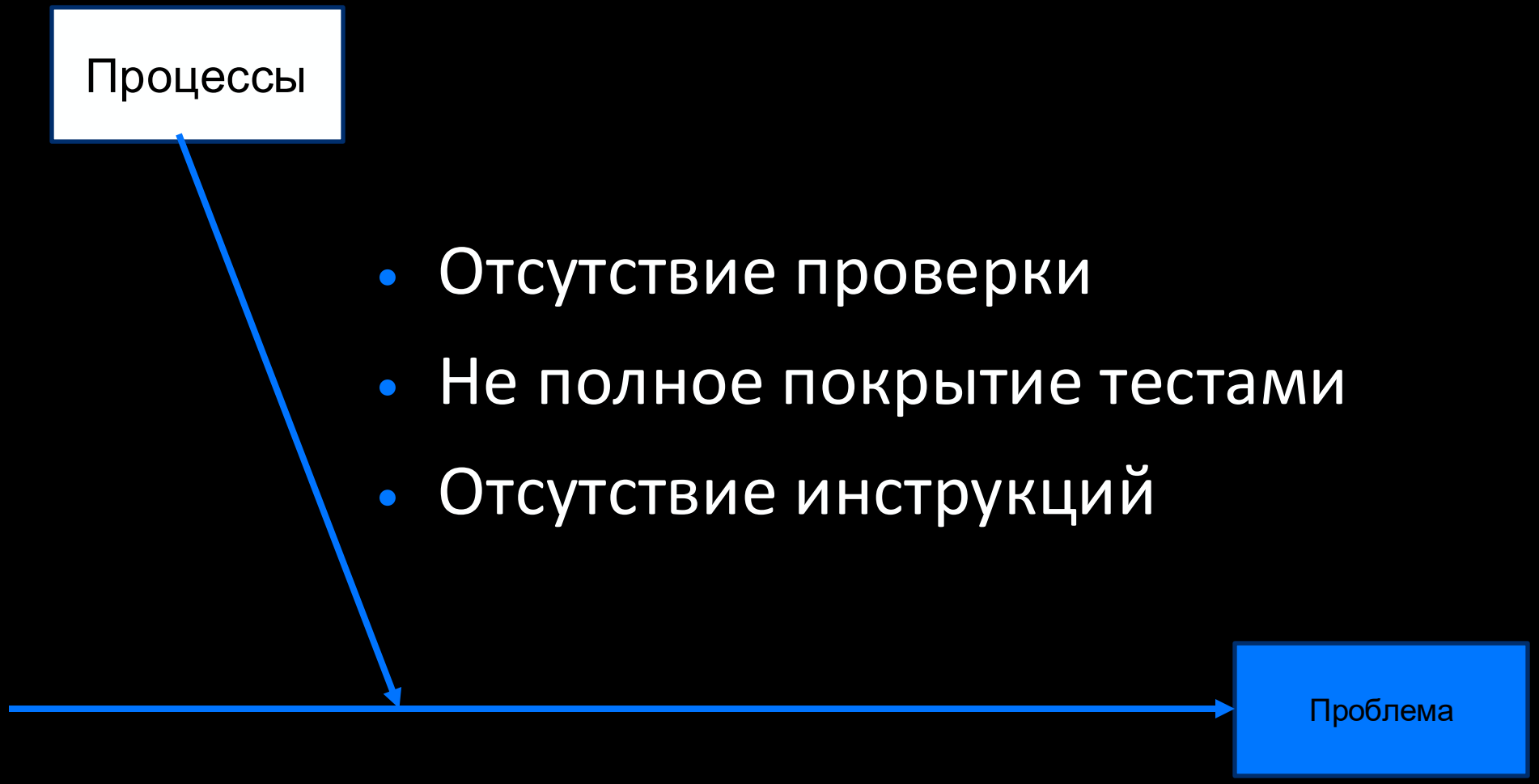
Подходит для быстрого анализа несложных проблем.

- Ограниченный поиск RC
- Субъективный результат
- Упрощенные выводы

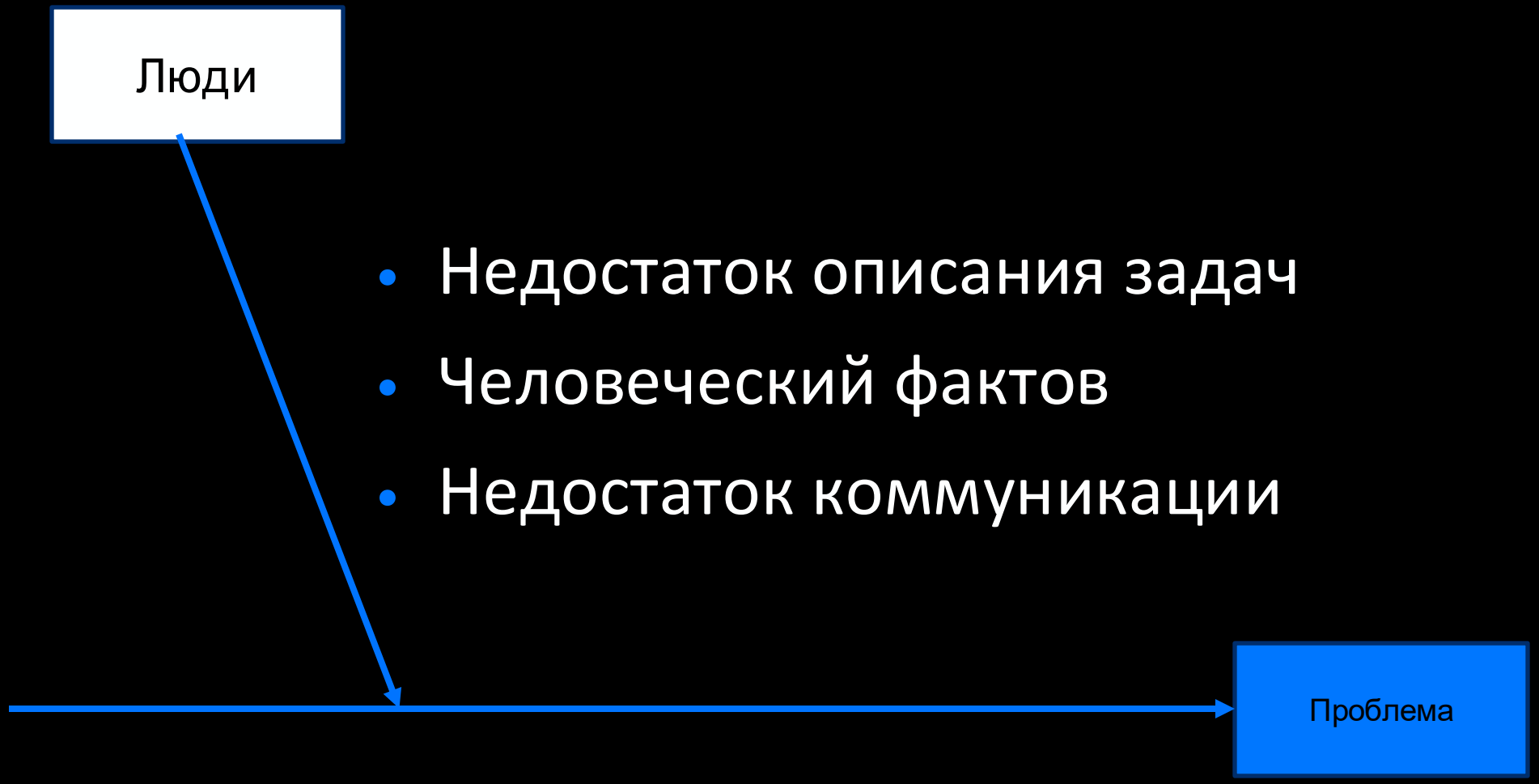
Fishbone Diagram



Fishbone Diagram

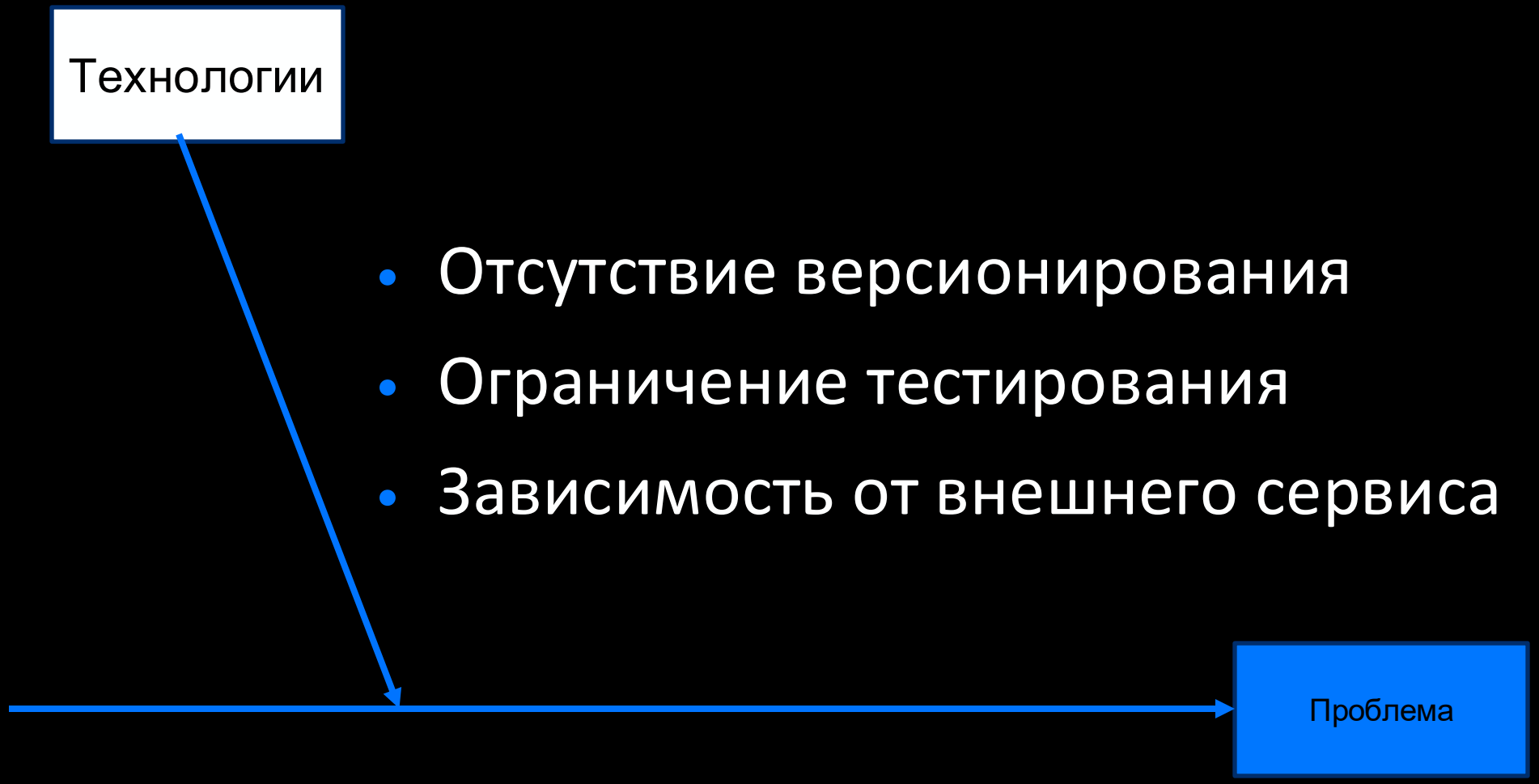


Fishbone Diagram



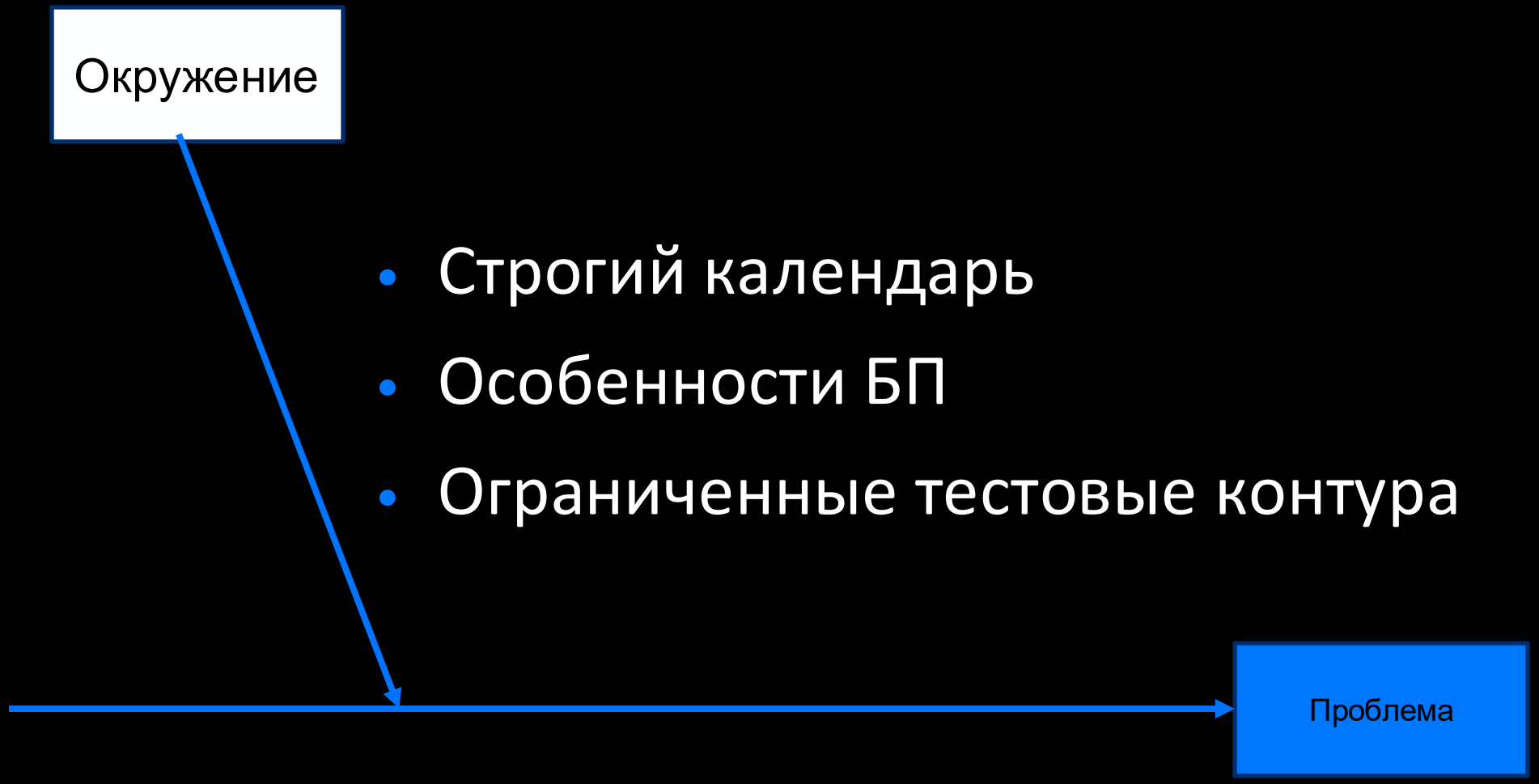
- Недостаток описания задач
- Человеческий фактов
- Недостаток коммуникации

Fishbone Diagram



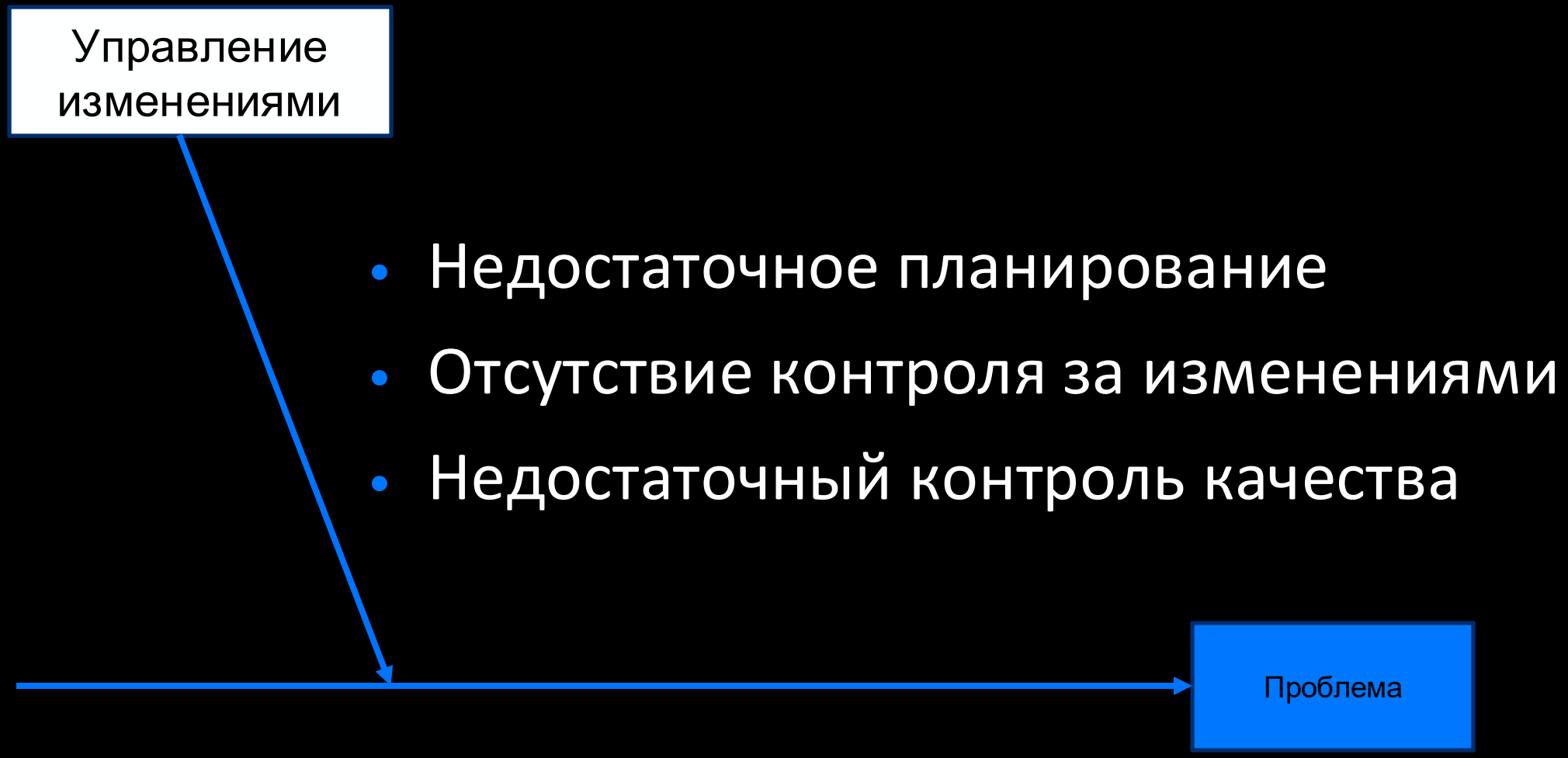
- Отсутствие версионирования
- Ограничение тестирования
- Зависимость от внешнего сервиса

Fishbone Diagram

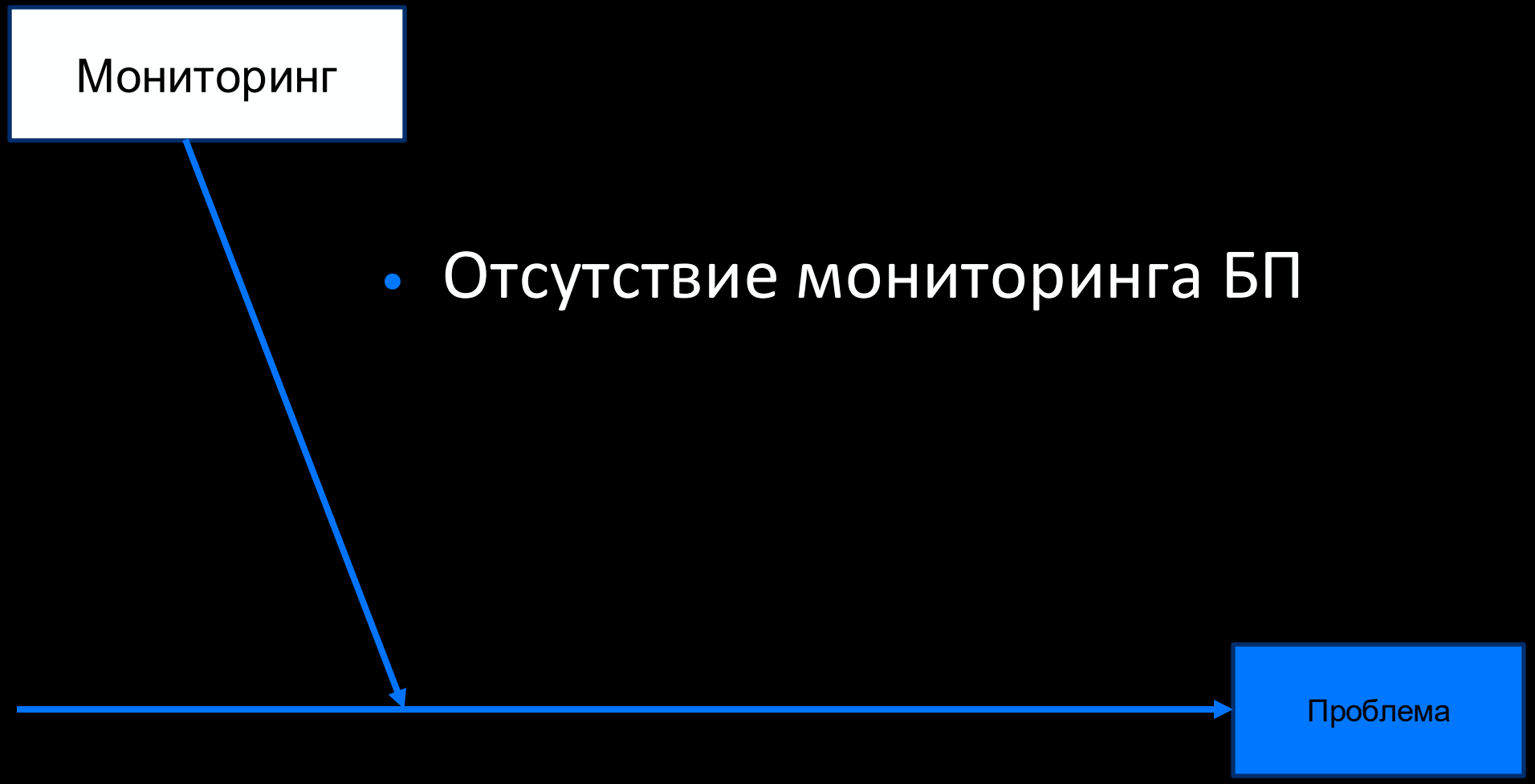


- Строгий календарь
- Особенности БП
- Ограниченные тестовые контура

Fishbone Diagram



Fishbone Diagram



- Отсутствие мониторинга БП

Root Cause

- Отсутствие поддержки переходящих процессов
- Сжатые сроки релизов
- Неактуальность инструкции для инженеров

Границы применимости

Подходит для системного анализа проблем в сложны системах

- Трудозатратный
- Зависит от команды

FMEA

- Определение компонентов
- Анализ вида отказов
- Оценка их последствий
- Разработка мер для минимизации риска

FMEA

- Ошибка при миграции сервисов
- Недоступность внешнего сервиса
- Ошибочные действия инженера

FMEA

Потенциальный отказ	Возможные причины	Последствия	Серьезность (S)	Вероятность (O)	Способность к обнаружению (D)	RPN
Ошибка при миграции процессов на новую версию	Отсутствие тестирования миграции	Дублирование переводов	9	7	4	252
Недоступность внешнего сервиса	Внешние зависимости	Прерывание процессов	8	6	5	240
Ошибочные действия инженера сопровождения	Некорректный ранбук	Дублирование переводов	8	5	3	120

FMEA

Потенциальный отказ	Возможные причины	Последствия	Серьезность (S)	Вероятность (O)	Способность к обнаружению (D)	RPN
Ошибка при миграции процессов на новую версию	Отсутствие тестирования миграции	Дублирование переводов	9	7	4	252
Недоступность внешнего сервиса	Внешние зависимости	Прерывание процессов	8	6	5	240
Ошибочные действия инженера сопровождения	Некорректный ранбук	Дублирование переводов	8	5	3	120

Root Cause

- Архитектурная ошибка
- Отсутствие обработки отказа внешнего сервиса
- Некорректные ранбуки

Границы применимости

Определение влияния отказов на систему

- Требуется большая экспертиза по системе
- Не учитываются человеческие факторы
- Трудозатратный

Что использовать?!

Полная картина инцидента

- Обновление процесса без автоматической миграции уже существующих
- Неполнота тестовых сценариев
- Отсутствие обработки отказа внешнего сервиса
- Отсутствие процессов мониторинга BPM

5 WHYS

- Быстро и просто
- Субъективные выводы

Fishbone

- Визуально-наглядно, применимо для сложных систем
- Сложность в реализации

FMEA + Fishbone

- Риск-ориентированный подход
- Комплексный анализ
- Большие трудозатраты

Что же выбираю я?!

Крутая цитата

Если проблема имеет решение,
то волноваться незачем. Если решения нет, то волноваться бессмысленна (с) Стэтхем

Спасибо
за внимание!