

SLA

ДРУГ ИЛИ ВРАГ
РАЗРАБОТЧИКА?

Григорий Кошелев
Контур

DevOps, 2021

Дисклеймер

Доклад о вымышленном инциденте
произошедшем в вымышленной системе
в вымышленной вселенной
(Незнайка на Луне)

Все совпадения являются
непреднамеренными и случайными

План

- Лунный мир и автоматизация
- Инцидент и хроника восстановления
- SLA и SLO
- Надёжность и факторы влияния
- Выводы

Shit happens

- Иногда что-то ломается (всё)
- Иногда надолго
- Иногда безвозвратно

<http://www.rbc.ru/economics/02/04/2016/56fff2759a79478904a38f73>

<http://www.alta.ru/news/43707/>

<http://www.rbc.ru/rbcfreenews/570133cd9a79473f7f5631b5>

Жизнь на Луне

По мотивам художественного произведения «Незнайка на Луне»

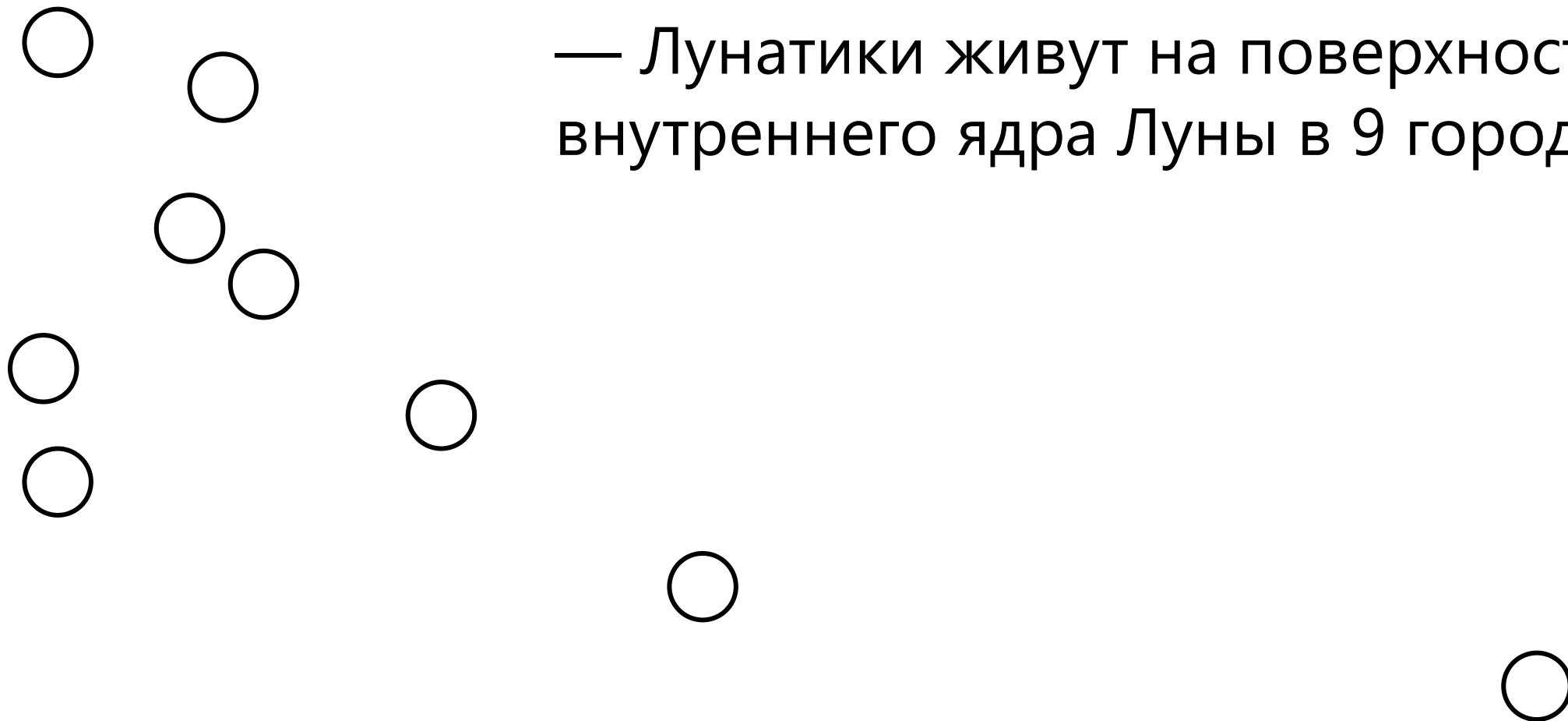
Немного об устройстве лунного мира

Немного об устройстве лунного мира

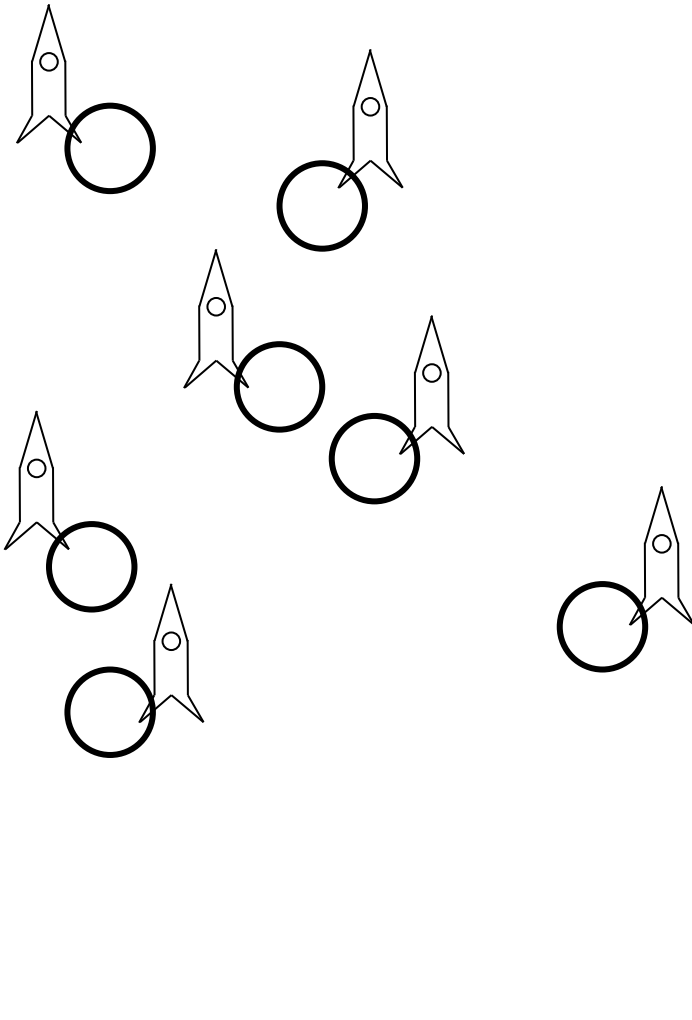
— Лунатики живут на поверхности
внутреннего ядра Луны в 9 городах

Немного об устройстве лунного мира

— Лунатики живут на поверхности
внутреннего ядра Луны в 9 городах

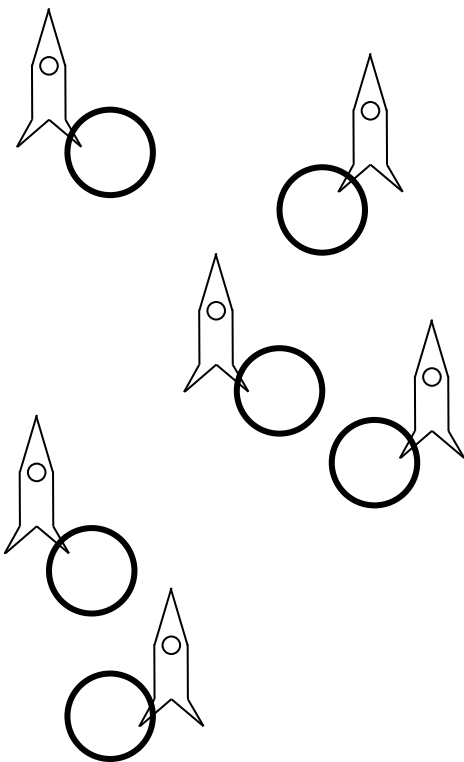


Немного об устройстве лунного мира



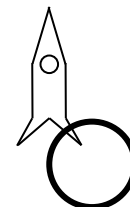
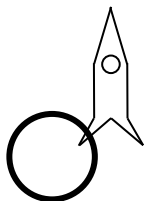
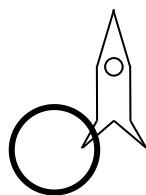
— В каждом городе расположен космодром, в который прилетают многоразовые ракеты

Немного об устройстве лунного мира

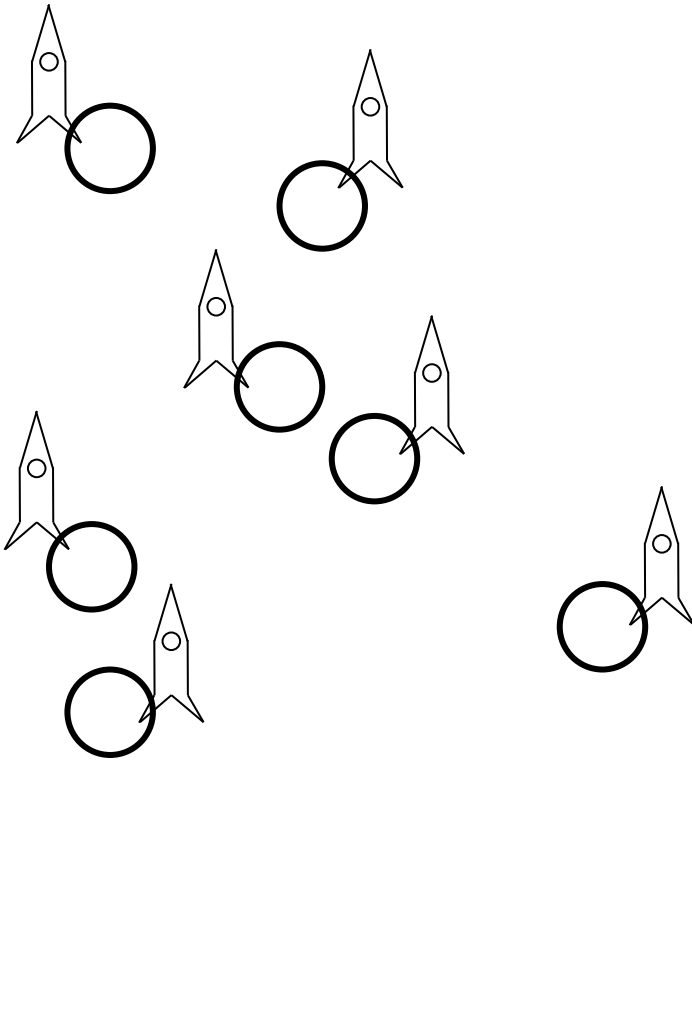


— В каждом городе расположен космодром, в который прилетают многоразовые ракеты

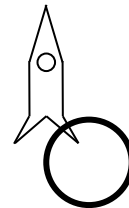
— В ракетах (помимо коротышек) возят товары



Немного об устройстве лунного мира



**Задача: научиться планировать и
контролировать заполняемость
ракет**



Немного об устройстве лунного мира

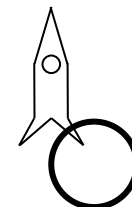
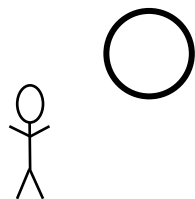
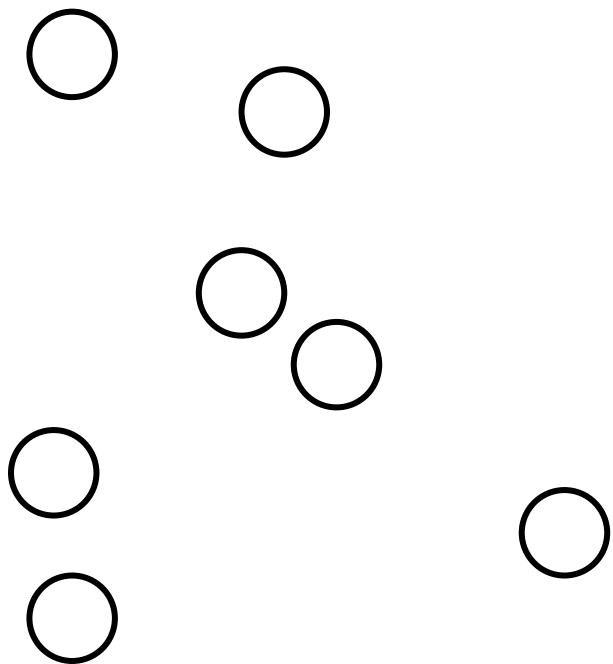
— Для контроля за товарооборотом организована
Фактическая Товарооборотная Служба (ФТС™)

Немного об устройстве лунного мира

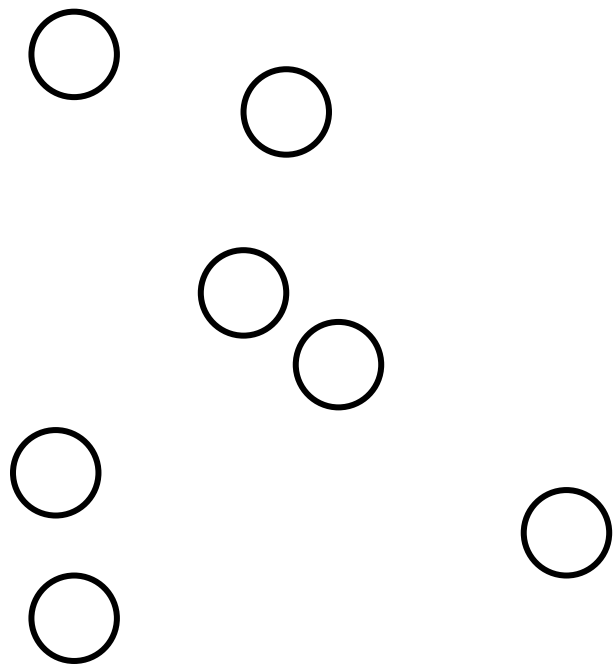
- Для контроля за товарооборотом организована Фактическая Товарооборотная Служба (ФТС™)
- Коротышки декларируют товары, импортируемые на Луну и экспортируемые с Луны

Карта Луны

— «Где карту Луны получали,
туда и идите»

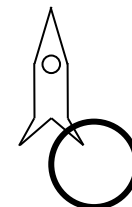
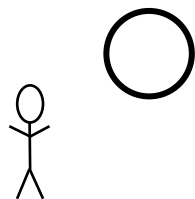


Карта Луны

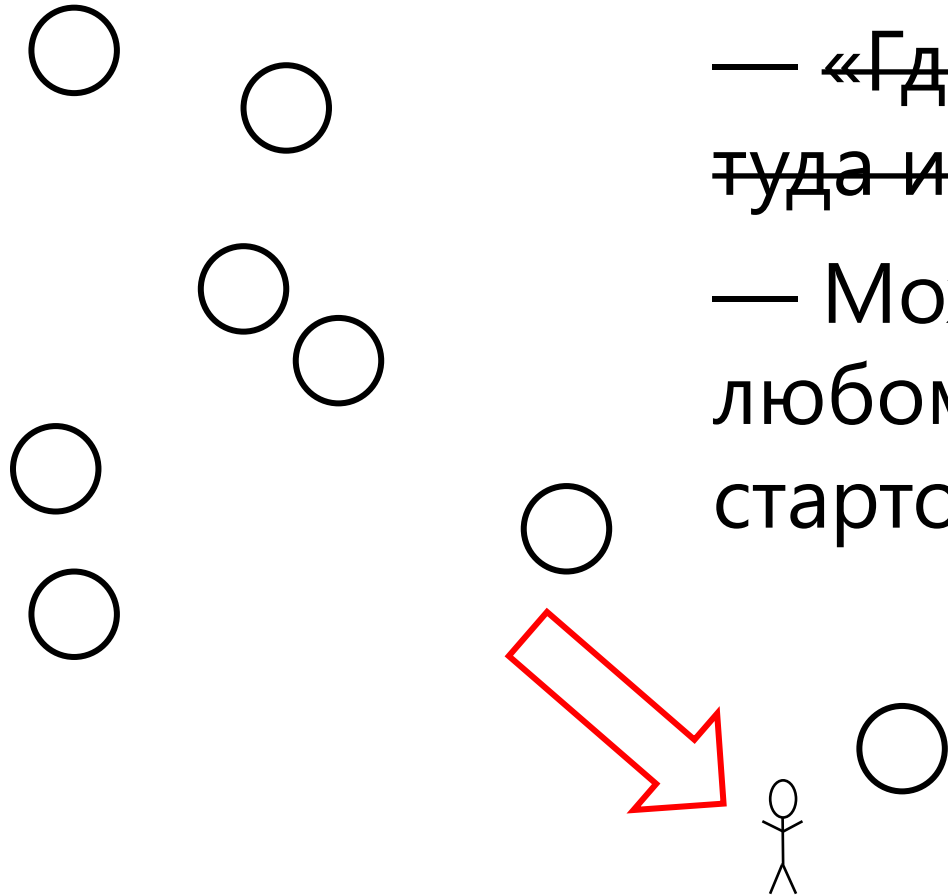


— ~~«Где карту Луны получали,
туда и идите»~~

— Можно подать декларацию в
любом филиале, независимо от
стартового космодрома ракеты



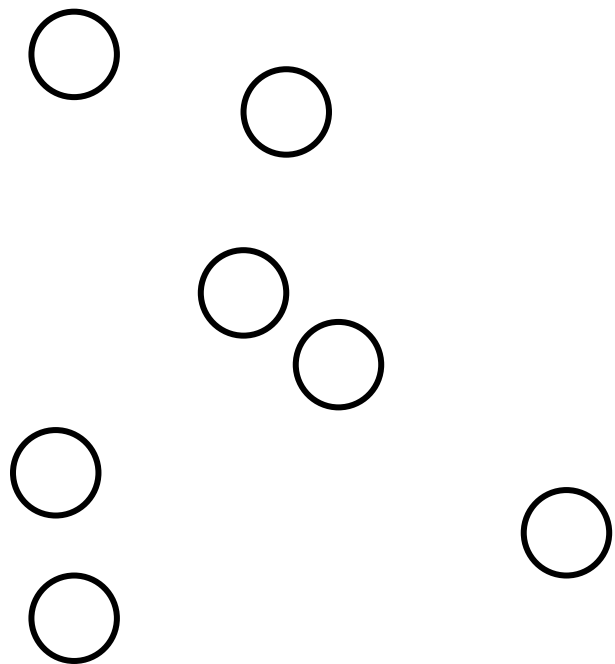
Карта Луны



— ~~«Где карту Луны получали,
туда и идите»~~

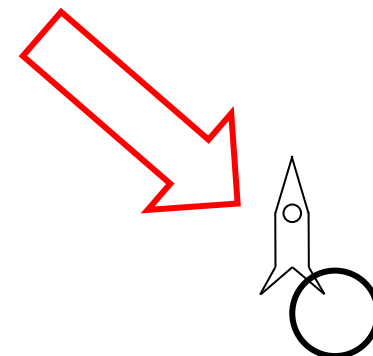
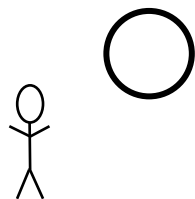
— Можно подать декларацию в
любом филиале, независимо от
стартового космодрома ракеты

Карта Луны

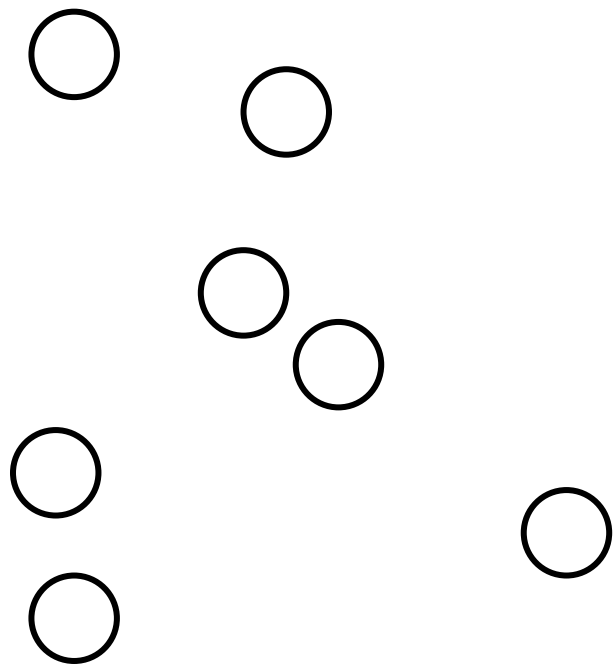


— ~~«Где карту Луны получали,
туда и идите»~~

— Можно подать декларацию в
любом филиале, независимо от
стартового космодрома ракеты

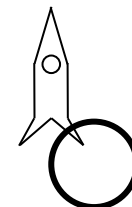
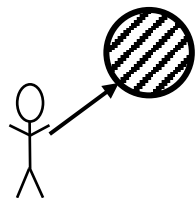


Карта Луны

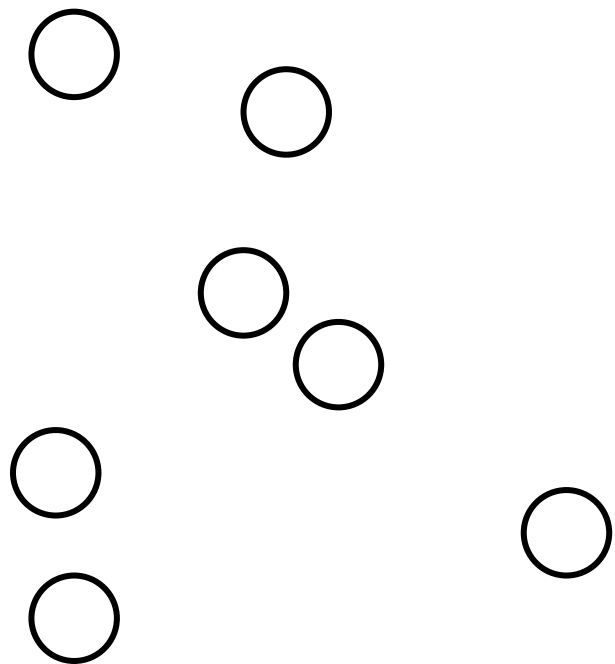


— ~~«Где карту Луны получали,
туда и идите»~~

— Можно подать декларацию в
любом филиале, независимо от
стартового космодрома ракеты

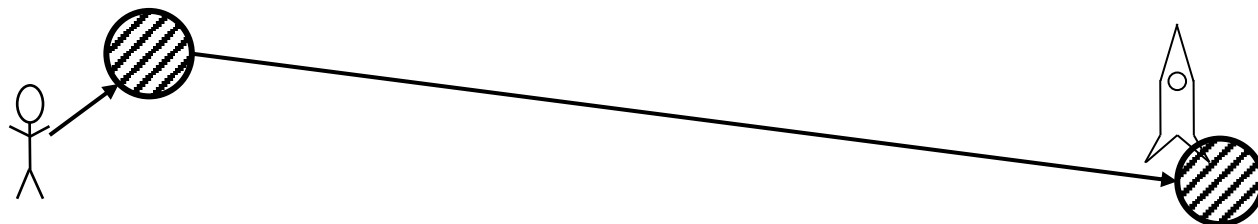


Карта Луны



— ~~«Где карту Луны получали,
туда и идите»~~

— Можно подать декларацию в
любом филиале, независимо от
стартового космодрома ракеты

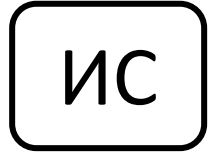


Архитектура

Архитектура

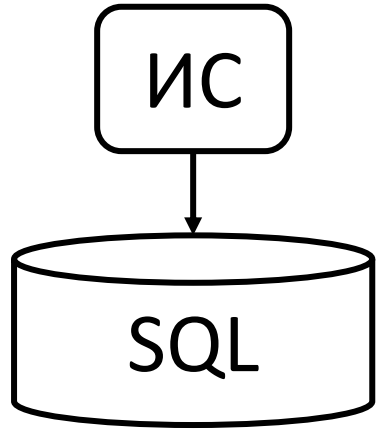
Всего 9 ЦОДов, в каждом:

Архитектура



Всего 9 ЦОДов, в каждом:
– крутится экземпляр ИС

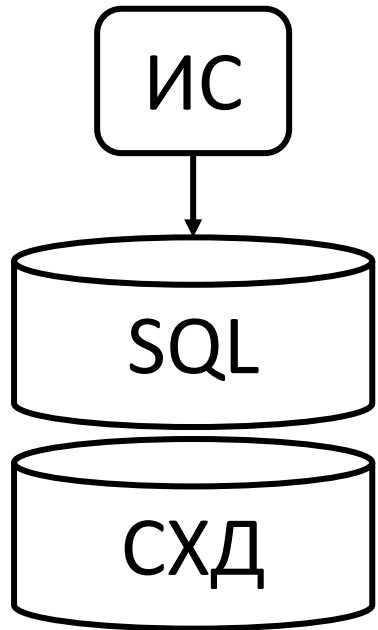
Архитектура



Всего 9 ЦОДов, в каждом:

- крутится экземпляр ИС
- «жирная» SQL-база

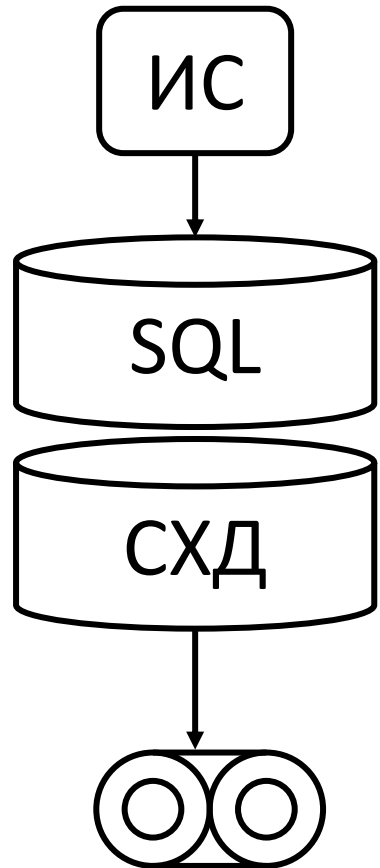
Архитектура



Всего 9 ЦОДов, в каждом:

- крутится экземпляр ИС
- «жирная» SQL-база
- под капотом отказоустойчивая СХД

Архитектура



Всего 9 ЦОДов, в каждом:

- крутится экземпляр ИС
- «жирная» SQL-база
- под капотом отказоустойчивая СХД
- БД периодически бэкапится на ленточные носители

Архитектура

— СУБД лицензирована только на один сервер (\$\$\$)

Архитектура

- СУБД лицензирована только на один сервер (\$\$\$)
- СХД поддерживает горячую замену дисков

Архитектура

- СУБД лицензирована только на один сервер (\$\$\$)
- СХД поддерживает горячую замену дисков
- Восстановление из redo logs после локальных сбоев встроенными средствами СУБД

Архитектура

- СУБД лицензирована только на один сервер (\$\$\$)
- СХД поддерживает горячую замену дисков
- Восстановление из redo logs после локальных сбоев встроенными средствами СУБД
- Возможность восстановления БД с ленточных носителей

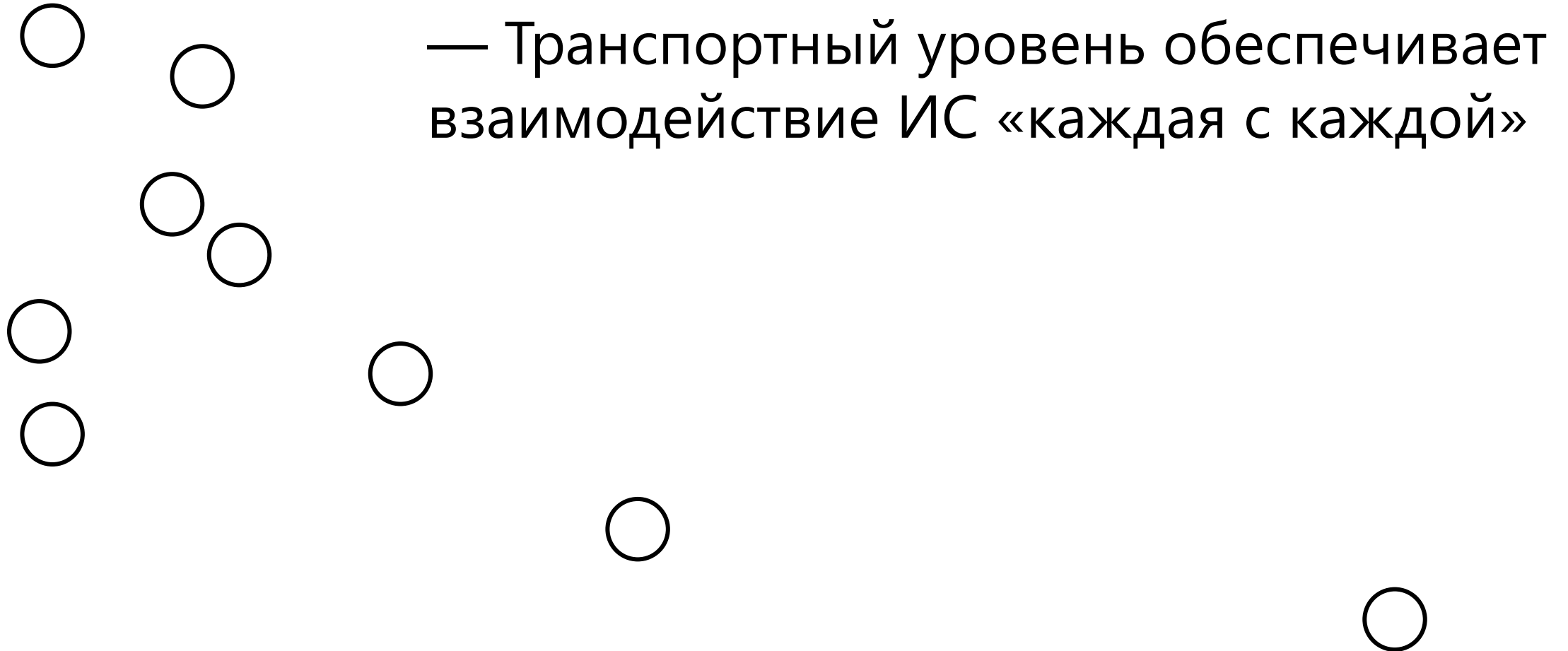
Архитектура

— Обработка сконцентрирована внутри одного ЦОДа

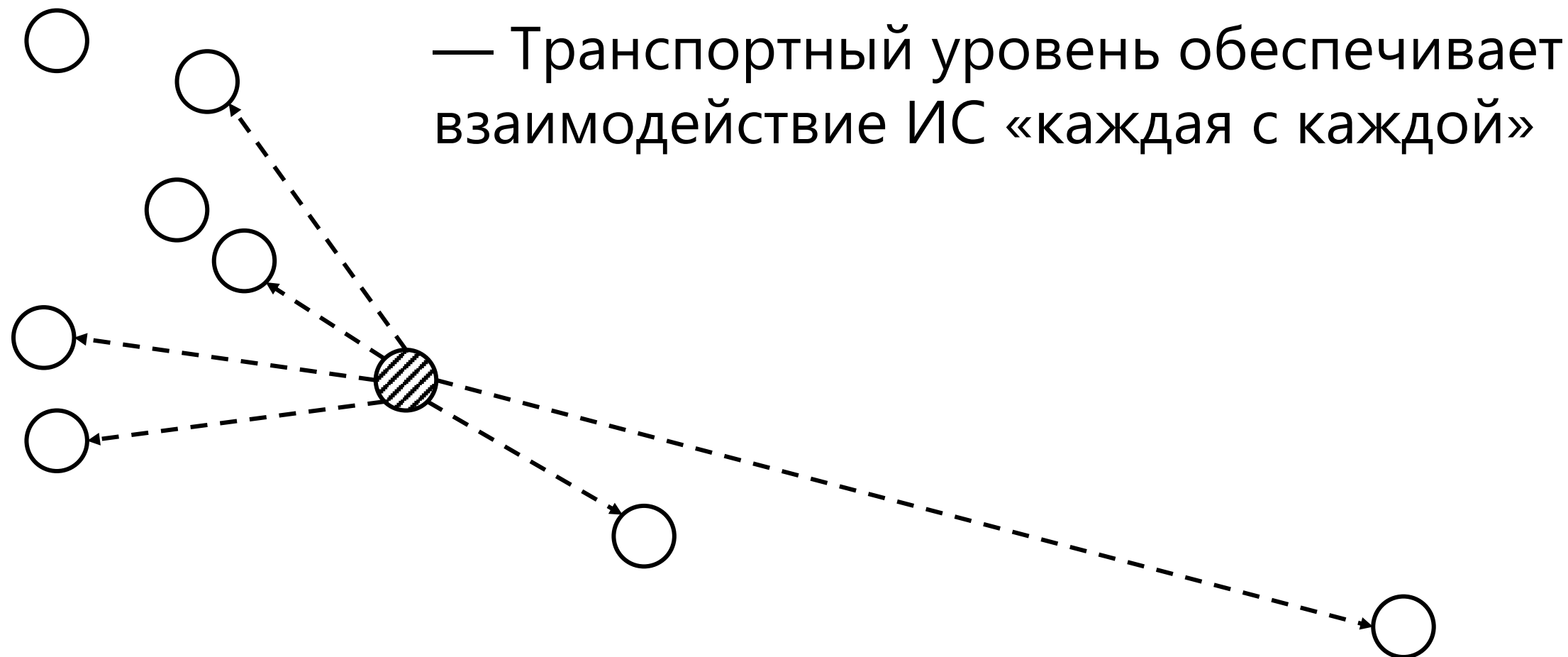
Архитектура

- Обработка сконцентрирована внутри одного ЦОДа
- Обмен данными между ИС, если коротышка декларирует товары из ракеты с другого космодрома

Архитектура



Архитектура



Инцидент

Shit happens

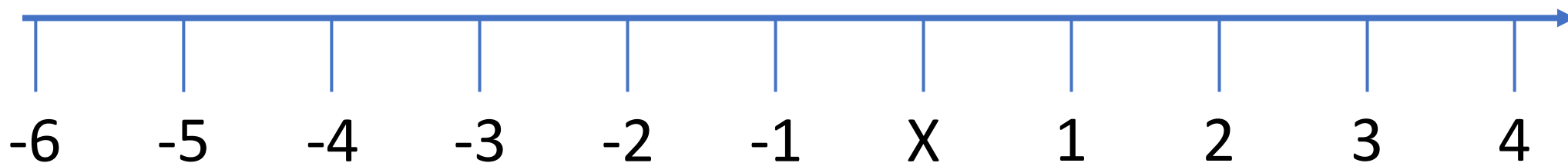
Хроника инцидента

X – день инцидента



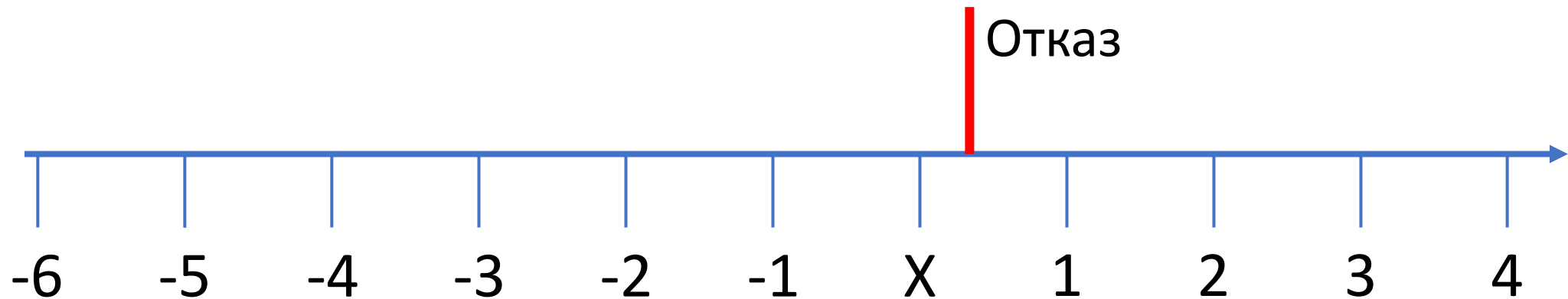
Хроника инцидента

X – день инцидента



Хроника инцидента

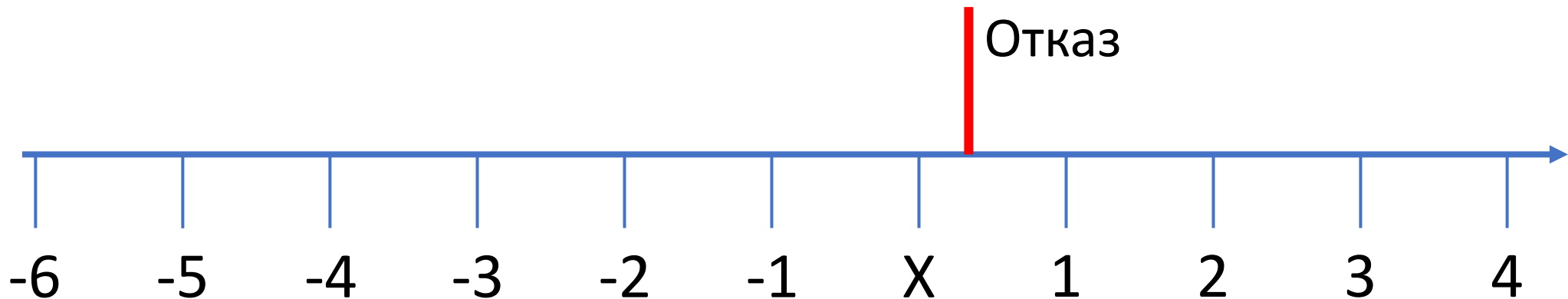
В СХД одного из ЦОДов сдох один из дисков



Хроника инцидента

В СХД одного из ЦОДов сдох один из дисков

— Инженер-коротышка заменил неисправный диск

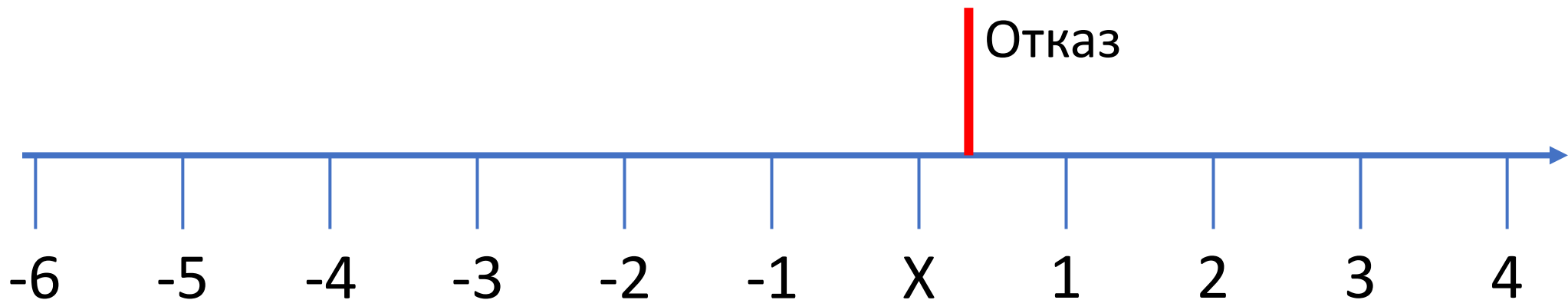


Хроника инцидента

В СХД одного из ЦОДов сдох один из дисков

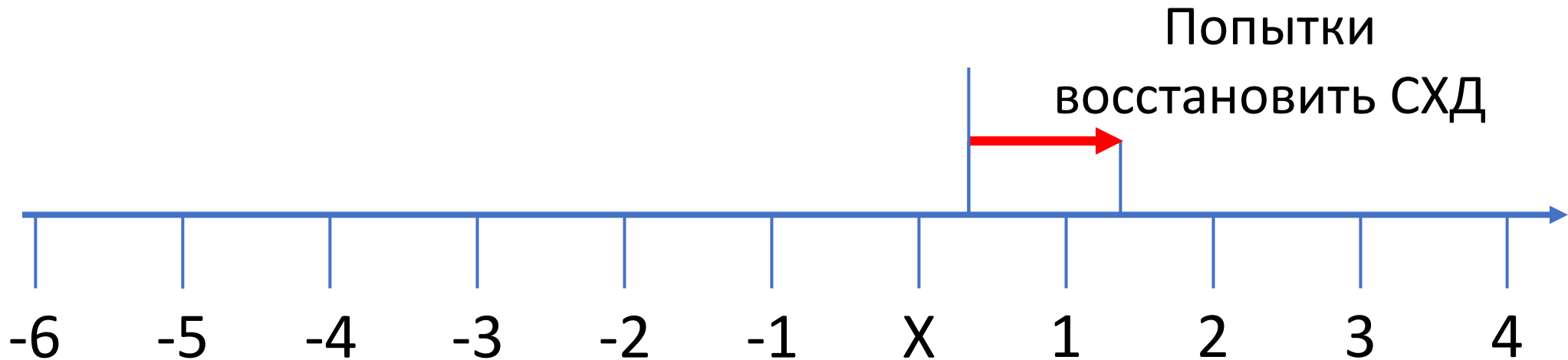
— Инженер-коротышка заменил неисправный диск

— Из-за неправильной инициализации потеряли 2 ТБ данных и развалили весь дисковый массив на 100 ТБ



Хроника инцидента

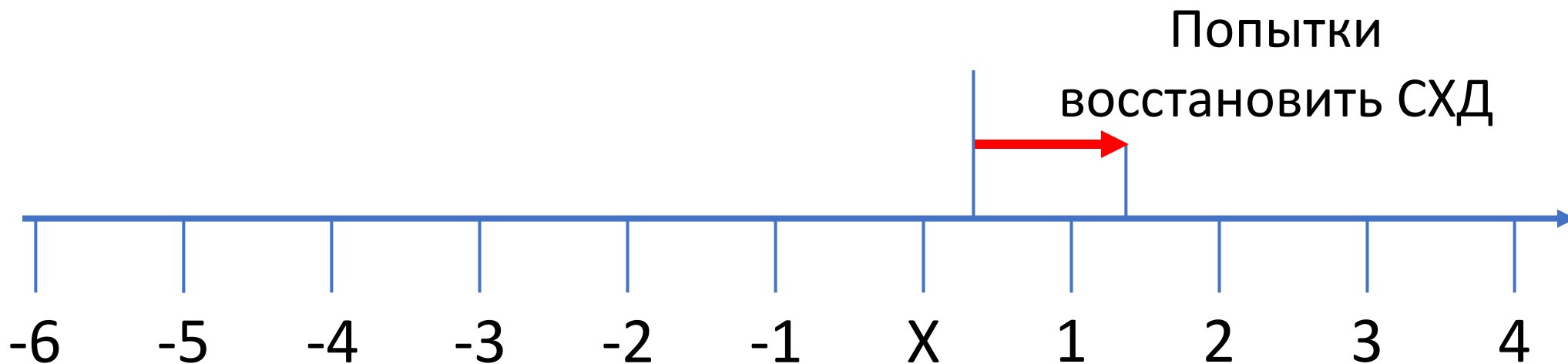
Попытки восстановить на уровне дисков



Хроника инцидента

Попытки восстановить на уровне дисков

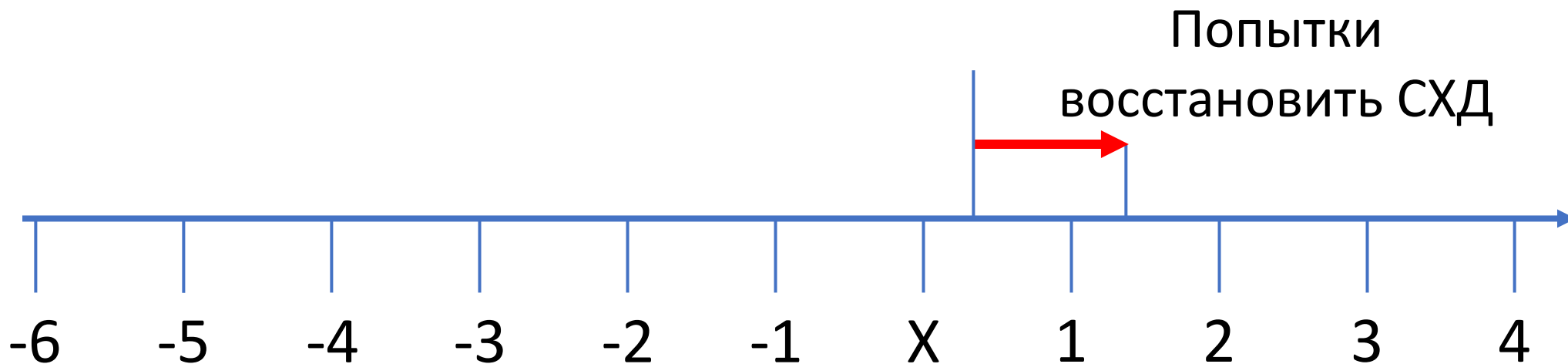
— Своими силами



Хроника инцидента

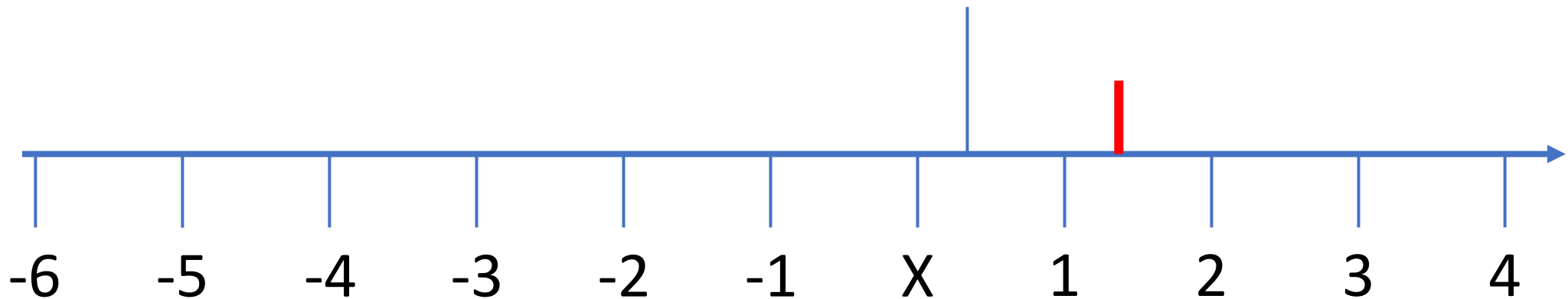
Попытки восстановить на уровне дисков

- Своими силами
- Обращение в саппорт к вендору



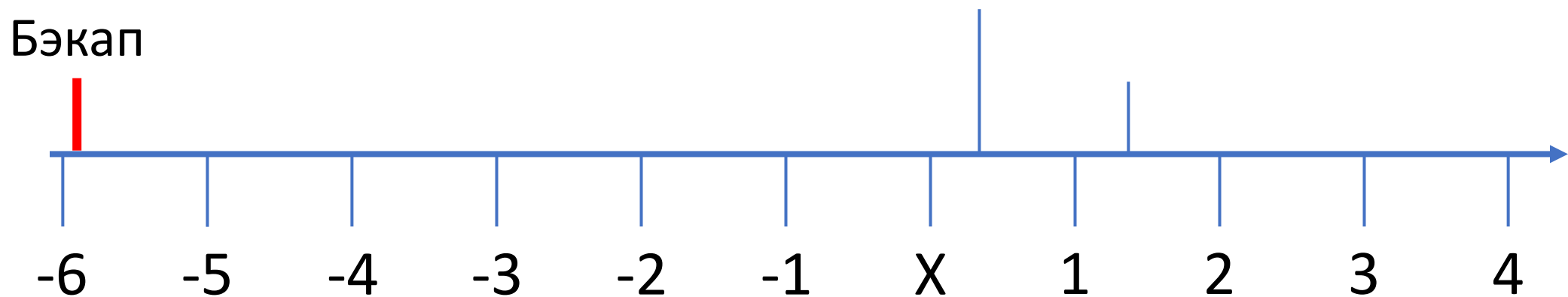
Хроника инцидента

Принято решение: восстановить БД из бэкапа



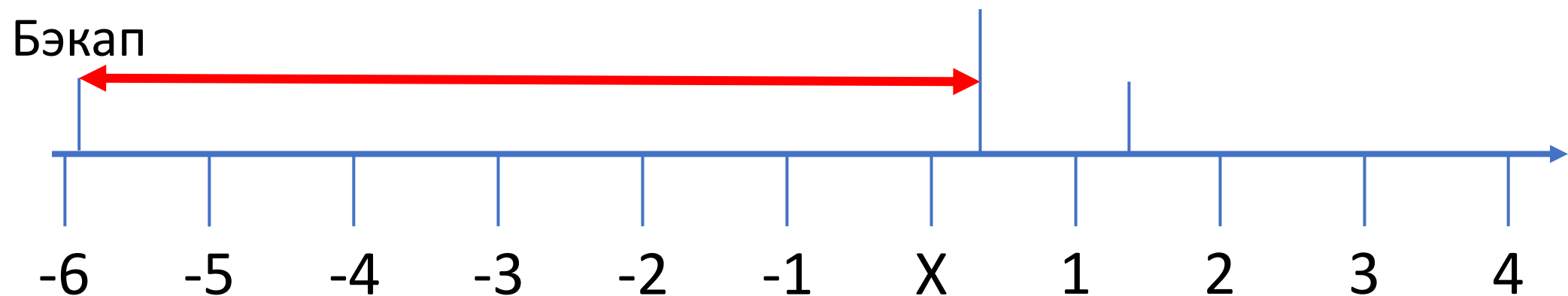
Хроника инцидента

Принято решение: восстановить БД из бэкапа



Хроника инцидента

Принято решение: восстановить БД из бэкапа
— Последний бэкап был за 6 дней до инцидента

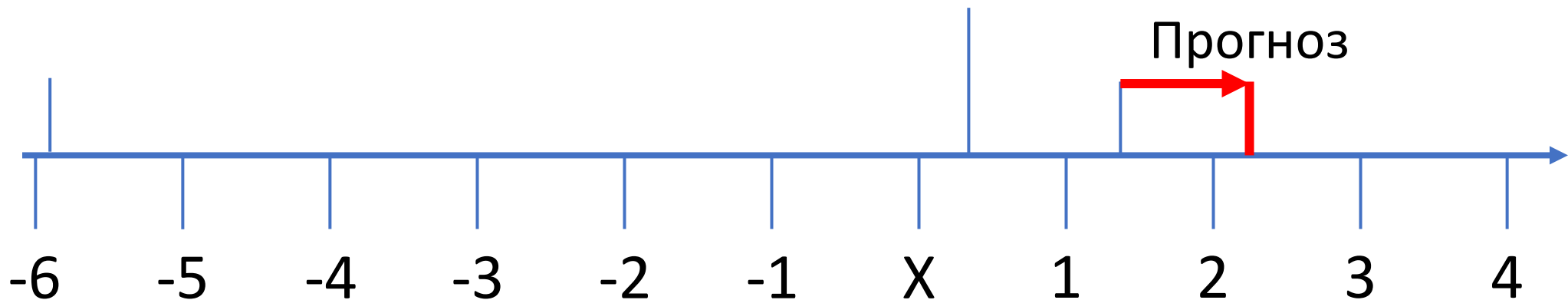


Хроника инцидента

Принято решение: восстановить БД из бэкапа

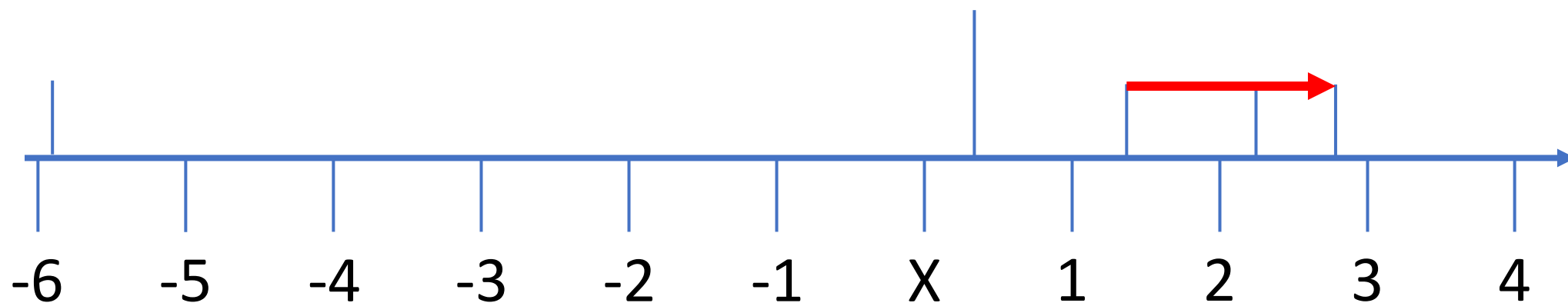
— Последний бэкап был за 6 дней до инцидента

— Прогноз: закончить к утру



Хроника инцидента

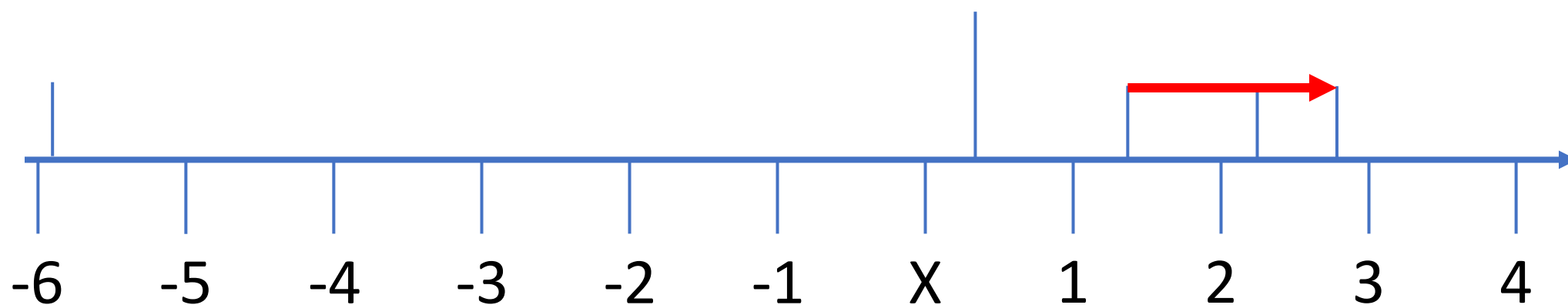
Восстановление БД из бэкапа



Хроника инцидента

Восстановление БД из бэкапа

— Более 60 ТБ

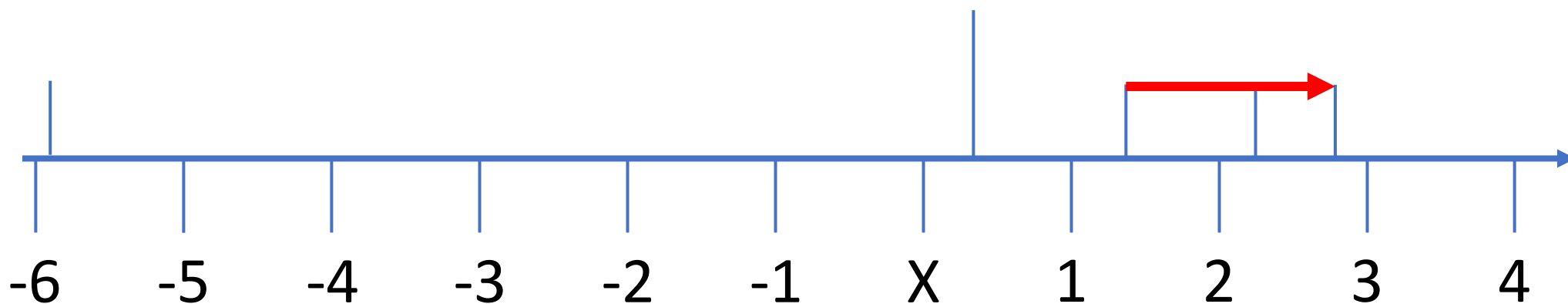


Хроника инцидента

Восстановление БД из бэкапа

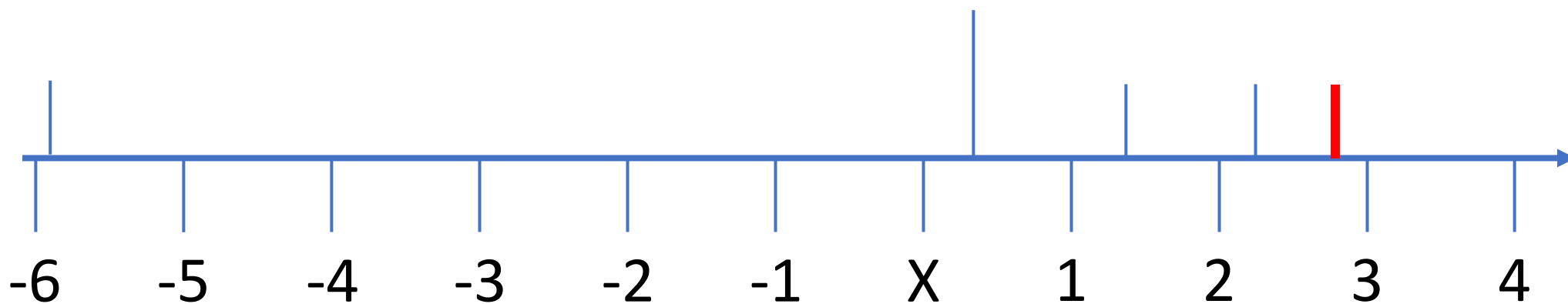
— Более 60 ТБ

— Процесс занял 30 часов



Хроника инцидента

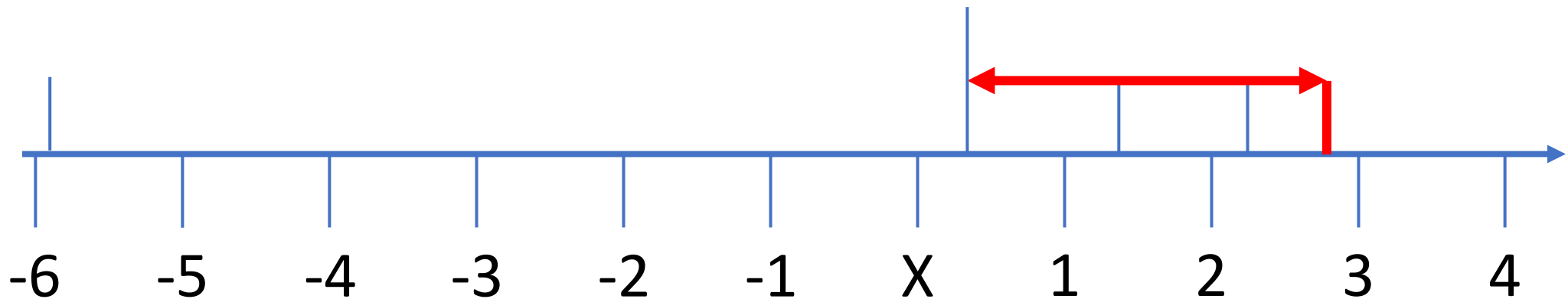
Что происходит?



Хроника инцидента

Что происходит?

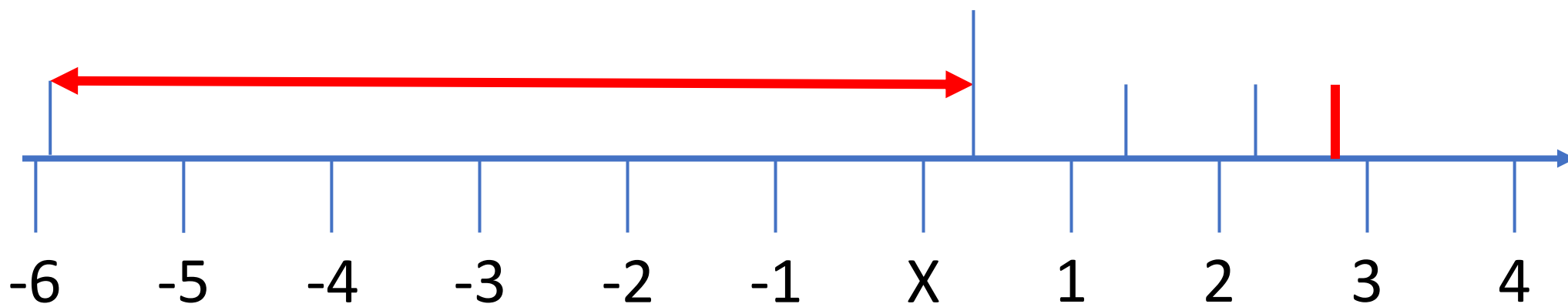
— Сервис не работает 2.5 дня



Хроника инцидента

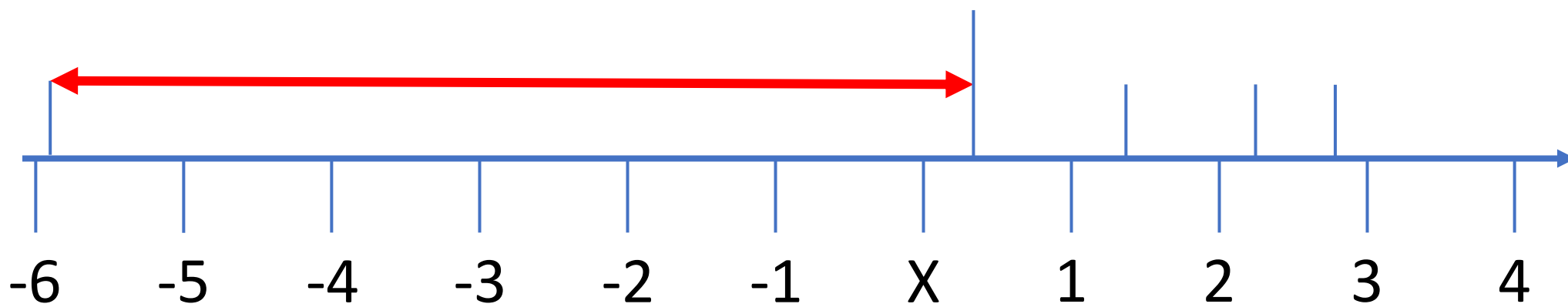
Что происходит?

- Сервис не работает 2.5 дня
- Потеряны данные за 6 дней



Хроника инцидента

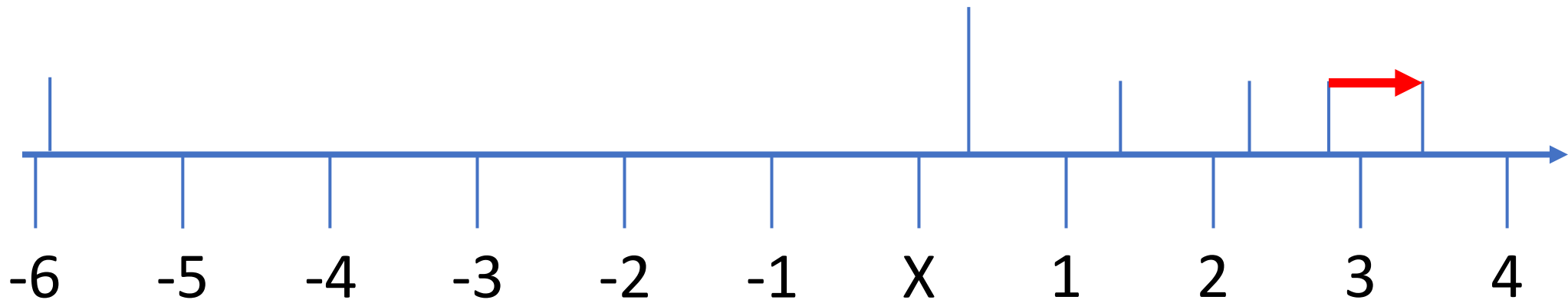
Повезло*: уцелели *redo logs*



Хроника инцидента

Повезло*: уцелели *redo logs*

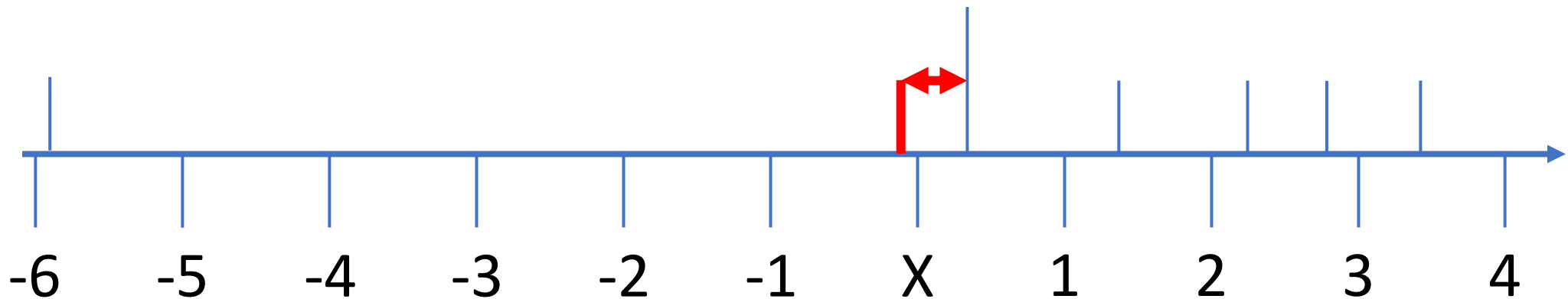
— Восстановление транзакций из redo logs



Хроника инцидента

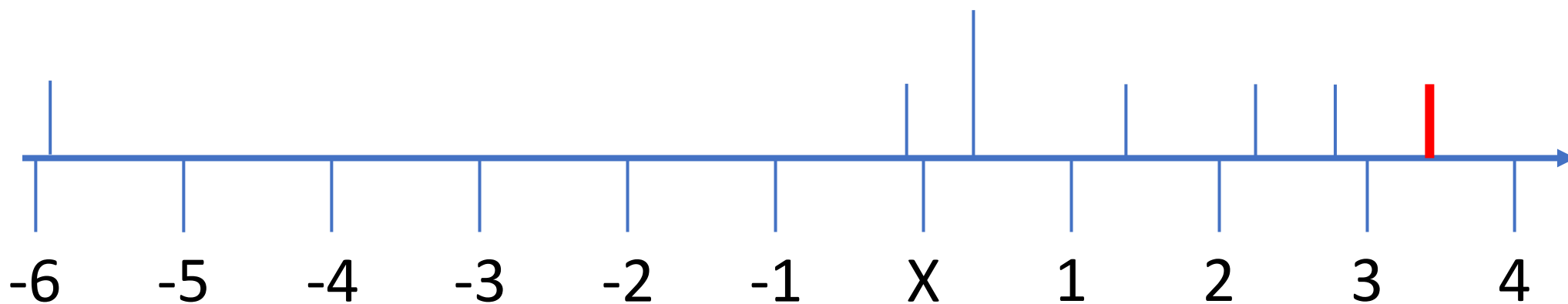
Повезло*: уцелели *redo logs*

- Восстановление транзакций из redo logs
- Безвозвратно утеряны данные за 11 часов**



Хроника инцидента

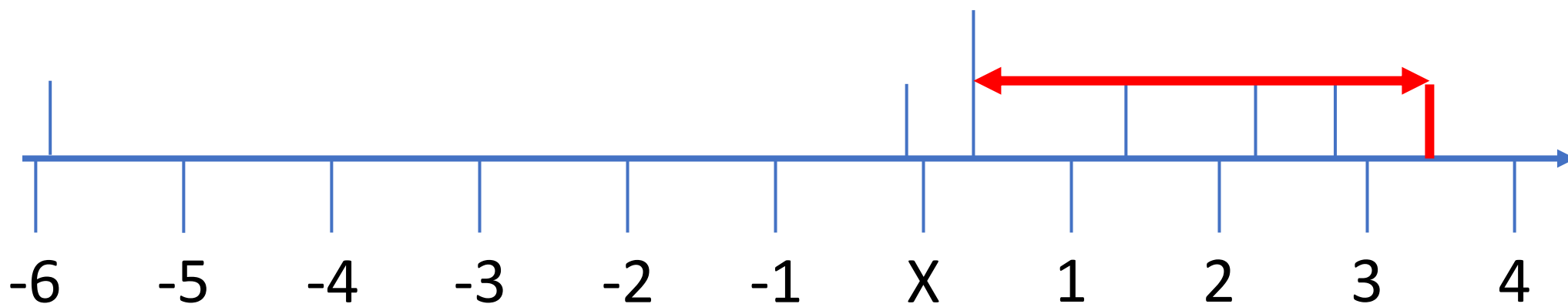
Что происходит?



Хроника инцидента

Что происходит?

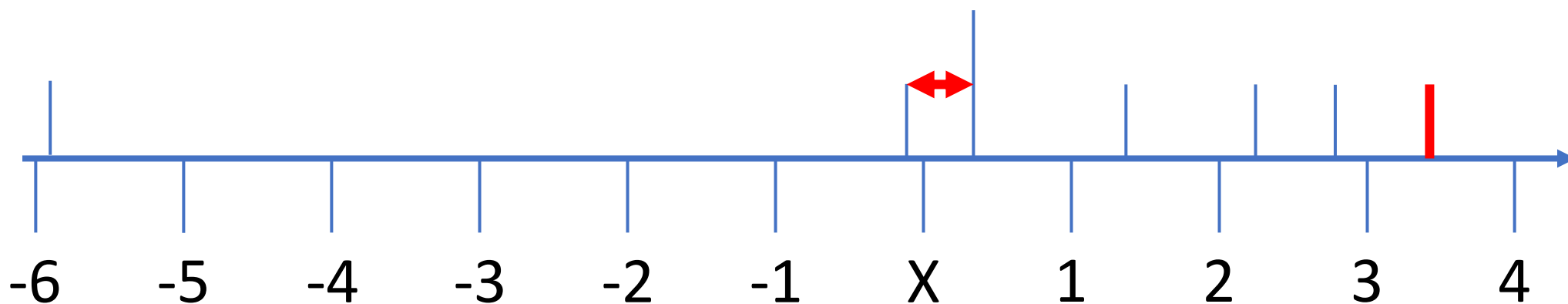
— Сервис не работал 3 дня



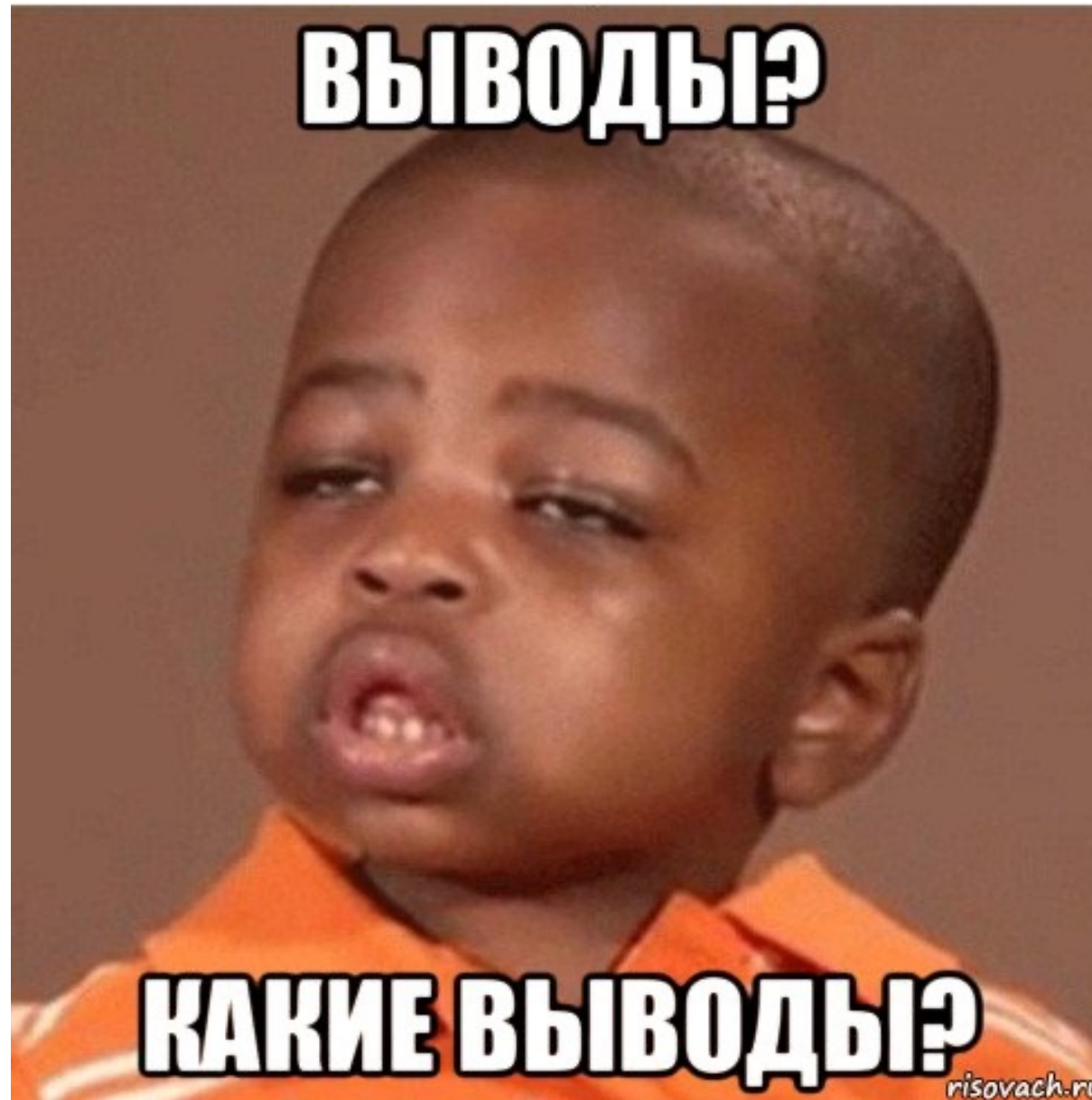
Хроника инцидента

Что происходит?

- Сервис не работал 3 дня
- Безвозвратно утеряны данные за 11 часов**



Выводы?



Нужен системный подход...

Service Level Agreement

Соглашение об уровне (качества) сервиса

SLA, чтобы...

SLA, чтобы...

А) Продать сервисы дорожке

SLA, чтобы...

А) Продать сервисы дорожке

В) Обставить конкурентов

SLA, чтобы...

- A) Продать сервисы дорожке
- B) Обставить конкурентов
- C) Удовлетворить запросы клиента

SLA, чтобы...

- A) Продать сервисы дорожке
- B) Обставить конкурентов
- C) Удовлетворить запросы клиента
- D) Быть в тренде (Google SRE Book)

SLA, чтобы...

A) Продать сервисы дорожке

B) Обставить конкурентов

C) Удовлетворить запросы клиента

D) Быть в тренде (Google SRE Book)

Вадим:

Что такое «качество»?

Вадим:

Что такое «качество»?

— **ГОСТ 15467-79**: «Качество — совокупность свойств продукции, обуславливающих её пригодность удовлетворять определённые потребности в соответствии с её назначением».

— **ISO 8402-86**: «Качество — совокупность свойств и характеристик продукции или услуги, которые придают им способность удовлетворять обусловленные или предполагаемые потребности потребителя».

Вадим:

Что такое «качество»?

— **ГОСТ 15467-79**: «Качество — совокупность свойств продукции, обуславливающих её пригодность удовлетворять определённые потребности в соответствии с её назначением».

— **ISO 8402-86**: «Качество — совокупность свойств и характеристик продукции или услуги, которые придают им способность удовлетворять обусловленные или предполагаемые потребности потребителя».

Структура SLA

- Формальный договор (определение Сервиса, стороны, сроки, финансы, ...)
- Формат работы Сервиса (24x7, 8x5, ...)
- Технологические перерывы (наличие, расписание)
- Предполагаемая нагрузка
- Процедура модернизации Сервиса
- Спецификация SLO
- Процесс формирования отчётов
- Зоны ответственности при эксплуатации
- Процесс улучшения SLA

Структура SLA

- **Формальный договор** (определение Сервиса, стороны, сроки, финансы, ...)
- Формат работы Сервиса (24x7, 8x5, ...)
- Технологические перерывы (наличие, расписание)
- Предполагаемая нагрузка
- Процедура модернизации Сервиса
- Спецификация SLO
- Процесс формирования отчётов
- Зоны ответственности при эксплуатации
- Процесс улучшения SLA

SLA — это касается каждого

SLA — это касается каждого

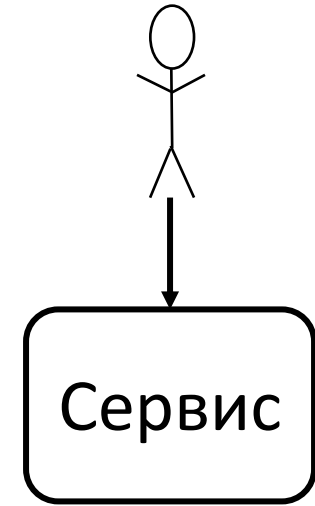
SLA — формирование ожиданий
от (качества) работы сервиса

"Уровни" SLA

SLA — формирование ожиданий
от (качества) работы сервиса

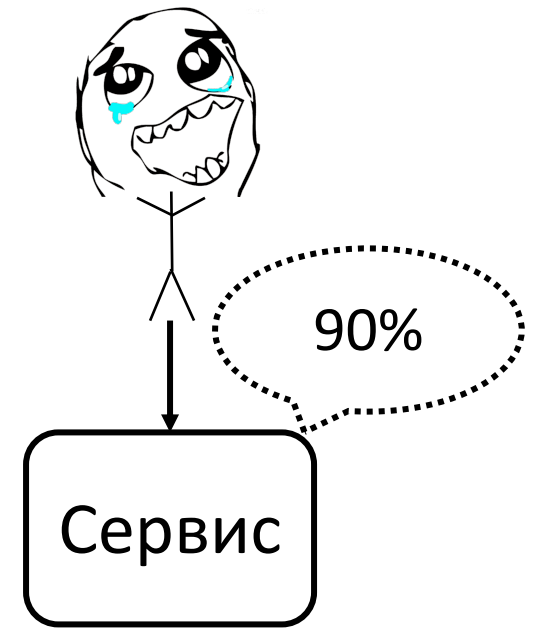
“Уровни” SLA

SLA — формирование ожиданий
от (качества) работы сервиса
— Для пользователей



"Уровни" SLA

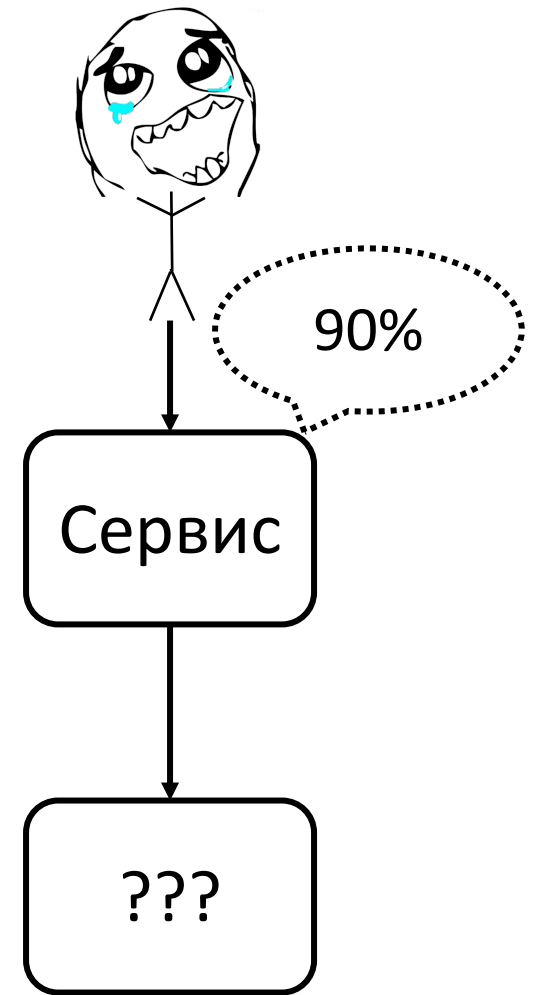
SLA — формирование ожиданий
от (качества) работы сервиса
— Для пользователей



"Уровни" SLA

SLA — формирование ожиданий от (качества) работы сервиса

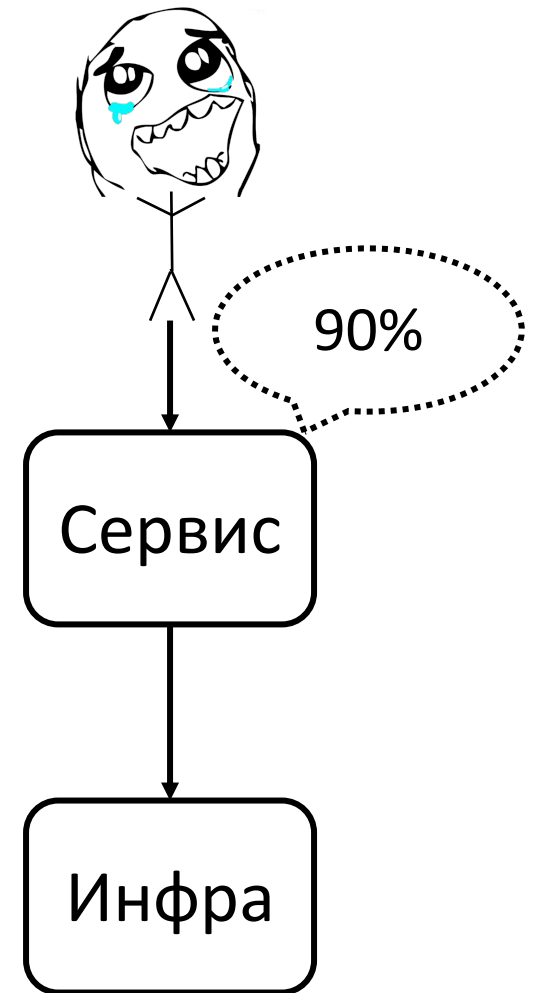
- Для пользователей
- Для других команд



"Уровни" SLA

SLA — формирование ожиданий от (качества) работы сервиса

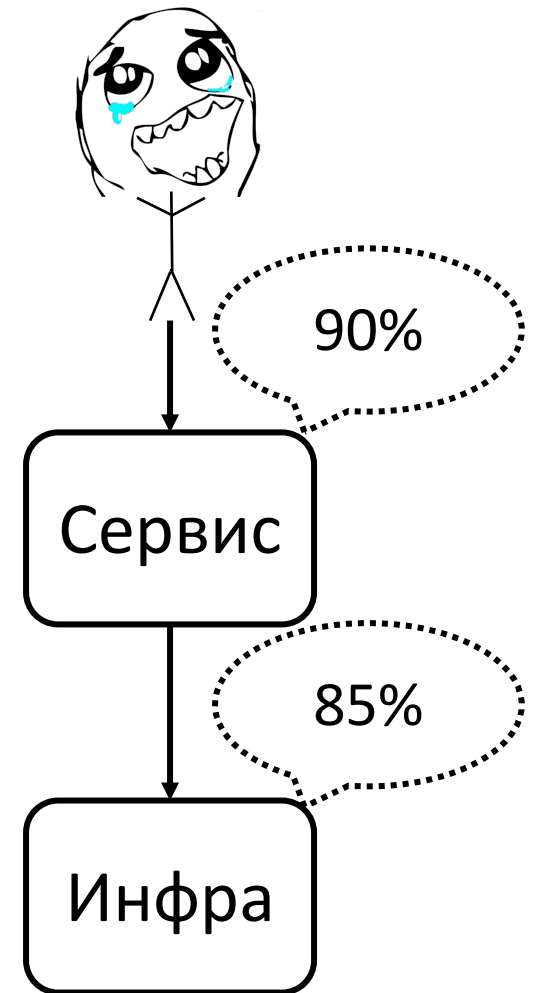
- Для пользователей
- Для других команд (инфраструктура)



"Уровни" SLA

SLA — формирование ожиданий от (качества) работы сервиса

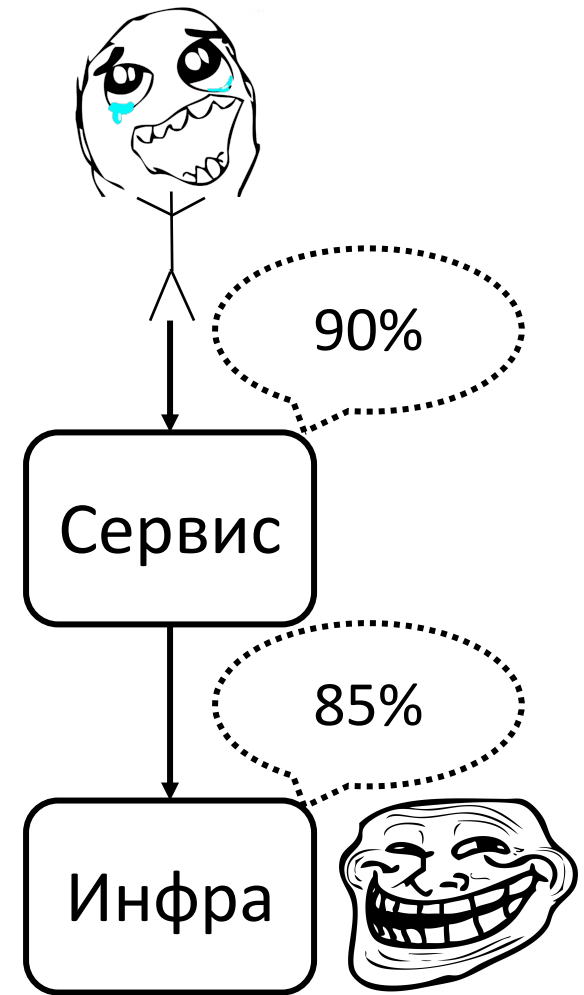
- Для пользователей
- Для других команд (инфраструктура)



"Уровни" SLA

SLA — формирование ожиданий от (качества) работы сервиса

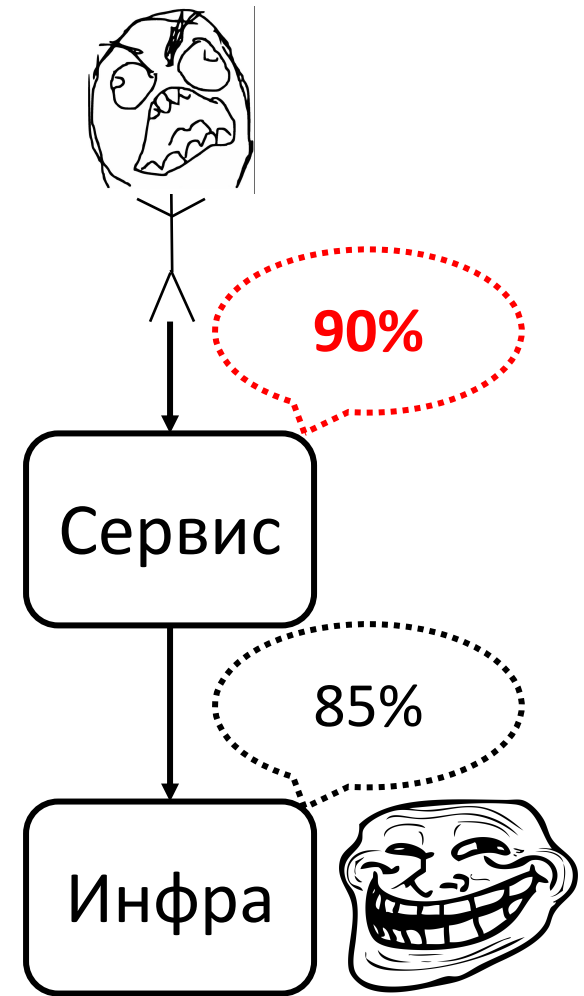
- Для пользователей
- Для других команд (инфраструктура)



"Уровни" SLA

SLA — формирование ожиданий от (качества) работы сервиса

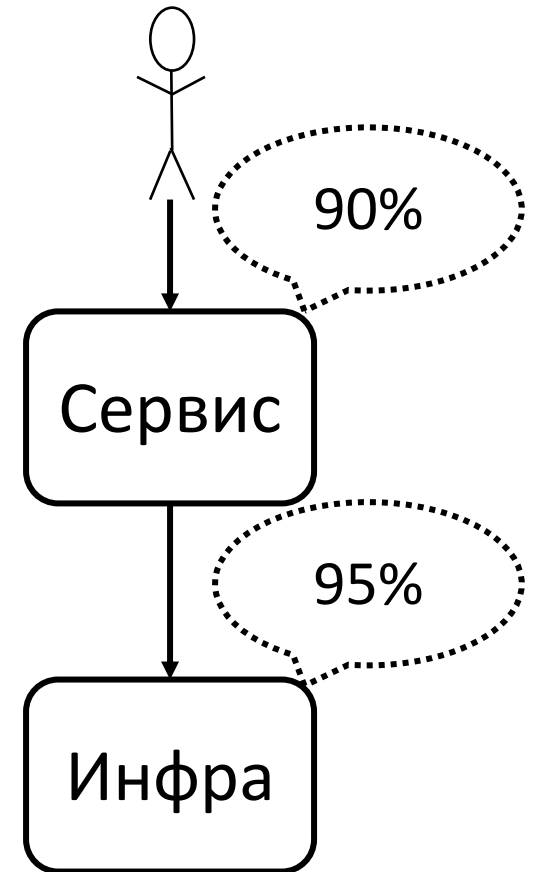
- Для пользователей
- Для других команд (инфраструктура)



“Уровни” SLA

SLA — формирование ожиданий от (качества) работы сервиса

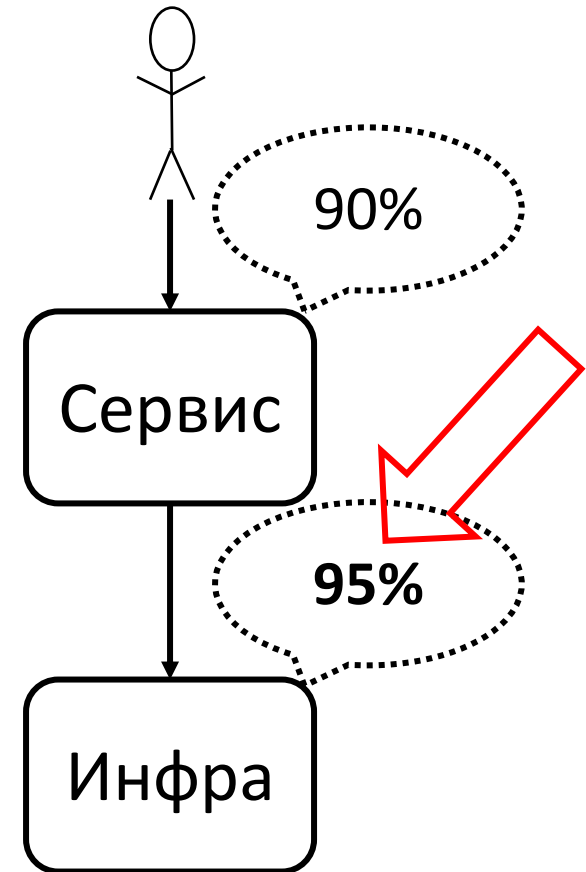
- Для пользователей
- Для других команд (инфраструктура)
- Для самих себя



“Уровни” SLA

SLA — формирование ожиданий от (качества) работы сервиса

- Для пользователей
- Для других команд (инфраструктура)
- Для самих себя

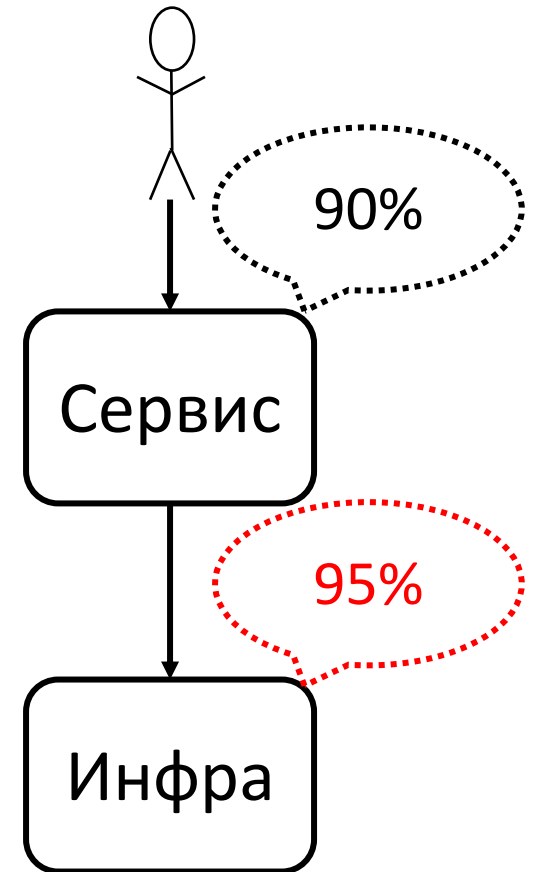


"Уровни" SLA

SLA — формирование ожиданий от (качества) работы сервиса

- Для пользователей
- Для других команд (инфраструктура)
- Для самих себя

Факан уже случился или пока нет?



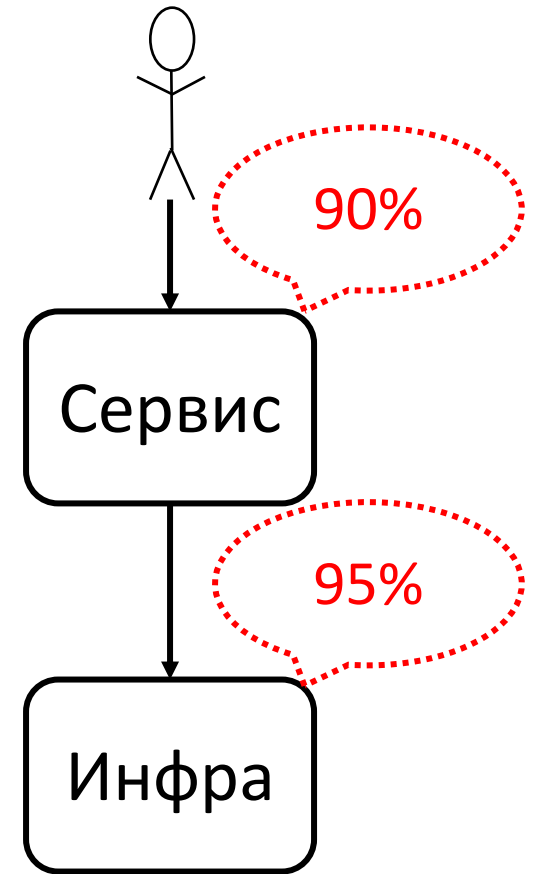
“Уровни” SLA

SLA — формирование ожиданий от (качества) работы сервиса

- Для пользователей
- Для других команд (инфраструктура)
- Для самих себя

Факан уже случился или пока нет?

Что делать, если случился?



"Уровни" SLA

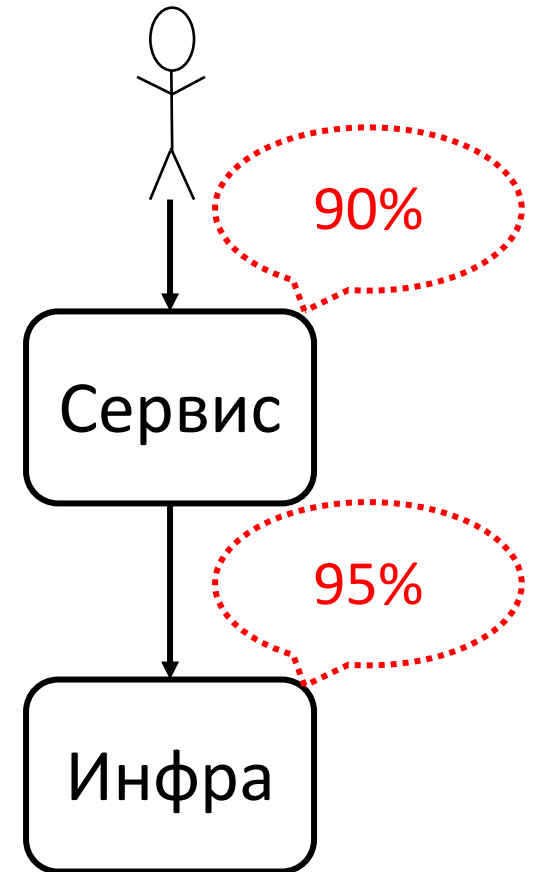
SLA — формирование ожиданий от (качества) работы сервиса

- Для пользователей
- Для других команд (инфраструктура)
- Для самих себя

Факан уже случился или пока нет?

Что делать, если случился?

А нас всех не уволят?



"Уровни" SLA

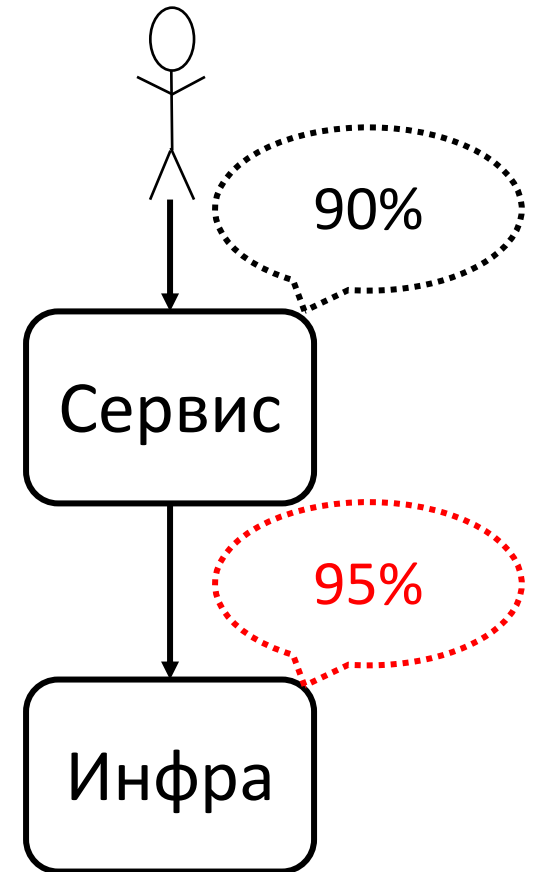
SLA — формирование ожиданий от (качества) работы сервиса

- Для пользователей
- Для других команд (инфраструктура)
- Для самих себя

Факан уже случился или пока нет?

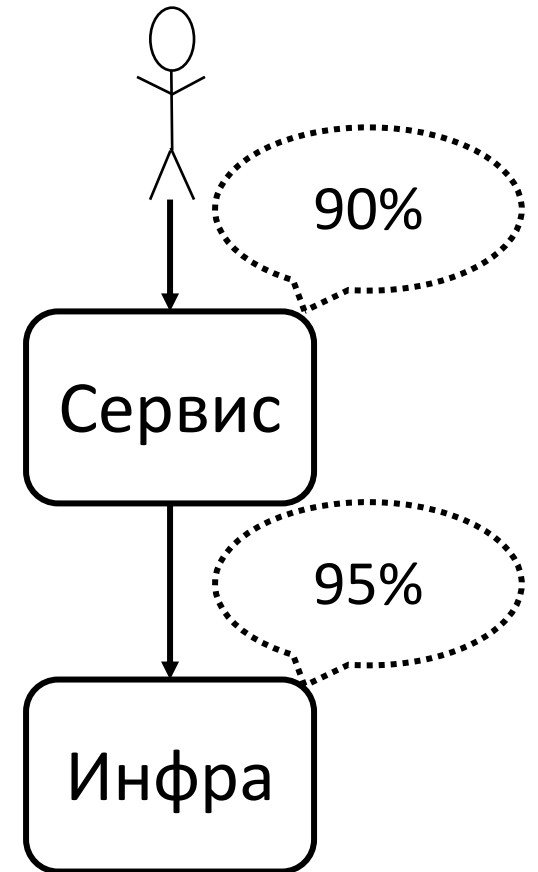
Что делать, если случился?

А нас всех не уволят? Что мы можем сделать?



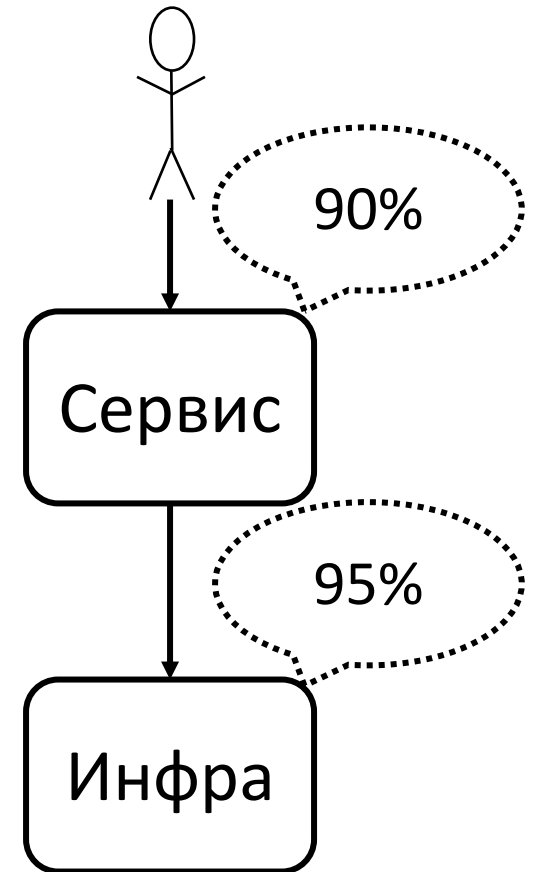
"Уровни" SLA

У инфраструктуры тоже есть уровни



"Уровни" SLA

У инфраструктуры тоже есть уровни
— ПО

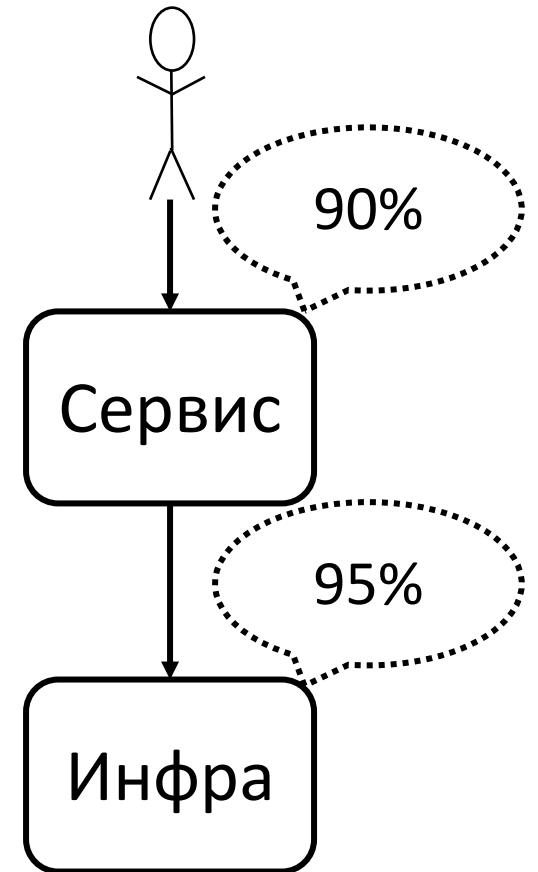


"Уровни" SLA

У инфраструктуры тоже есть уровни

— ПО

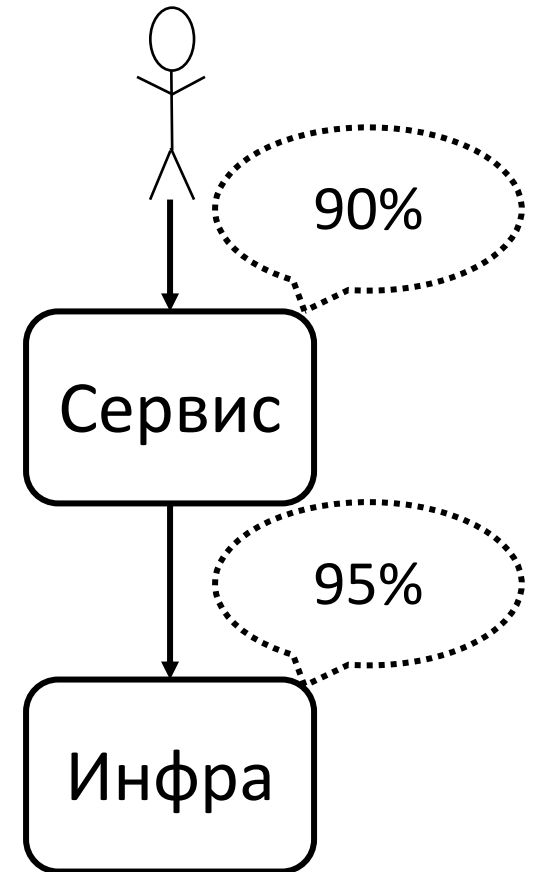
— Железо



"Уровни" SLA

У инфраструктуры тоже есть уровни

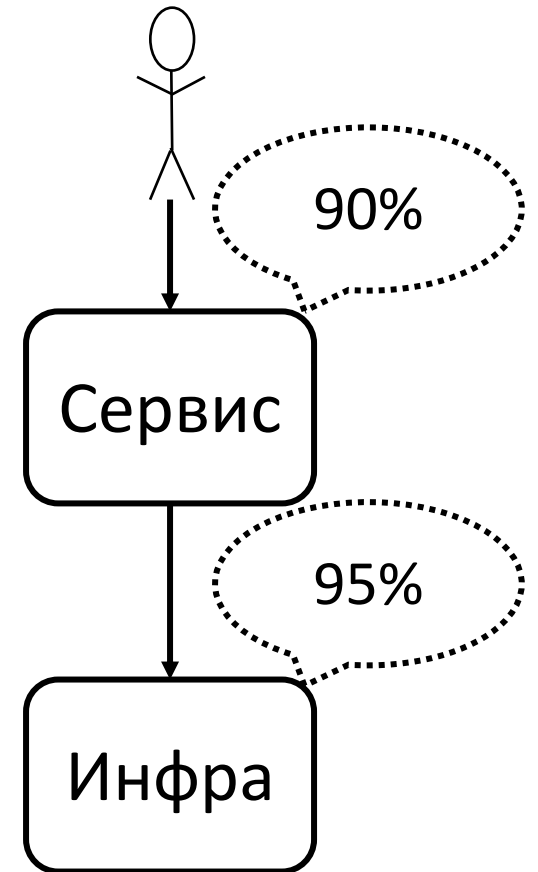
- ПО
- Железо
- Сеть



"Уровни" SLA

У инфраструктуры тоже есть уровни

- ПО
- Железо
- Сеть
- Люди



Структура SLA

- Формальный договор (определение Сервиса, стороны, сроки, финансы, ...)
- Формат работы Сервиса (24x7, 8x5, ...)
- Технологические перерывы (наличие, расписание)
- Предполагаемая нагрузка
- Процедура модернизации Сервиса
- **Спецификация SLO**
- Процесс формирования отчётов
- Зоны ответственности при эксплуатации
- Процесс улучшения SLA

Service Level Objective

Целевой уровень (качества) сервиса

SLOs

SLOs

Повторяемые

– Repeatable

SLOs

Повторяемые
Измеримые

- Repeatable
- Measurable

SLOs

Повторяемые

Измеримые

Значимые

– Repeatable

– Measurable

– Meaningful

SLOs

Повторяемые

– Repeatable

Измеримые

– Measurable

Значимые

– Meaningful

Достижимые

– Attainable

SLOs

Повторяемые

– Repeatable

Измеримые

– Measurable

Значимые

– Meaningful

Достижимые

– Attainable

Управляемые

– Controllable

Качественные характеристики

Качественные характеристики

Безопасность – Security

Качественные характеристики

Безопасность

– Security

Надёжность

– Reliability

Качественные характеристики

Безопасность

– Security

Надёжность

– Reliability

Производительность

– Performance

Качественные характеристики

Безопасность

– Security

Надёжность

– Reliability

Производительность

– Performance

Поддерживаемость

– Maintainability

Надёжность

Надёжность

Устойчивость к высоким нагрузкам

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Восстанавливаемость

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Восстанавливаемость

Целостность данных

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Восстанавливаемость

Целостность данных

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Восстанавливаемость

Целостность данных

Избыточность — Redundancy

Холодный резерв	– Cold Standby
Тёплый резерв	– Warm Standby
Горячий резерв	– Hot Standby
С балансировкой	– Load Balanced

Избыточность — Redundancy

Холодный резерв

– Cold Standby

Тёплый резерв

– Warm Standby

Горячий резерв

– Hot Standby

С балансировкой

– Load Balanced

Избыточность — Redundancy

Холодный резерв

– Cold Standby

Тёплый резерв

– **Warm Standby**

Горячий резерв

– Hot Standby

С балансировкой

– Load Balanced

Избыточность — Redundancy

Холодный резерв

– Cold Standby

Тёплый резерв

– Warm Standby

Горячий резерв

– **Hot Standby**

С балансировкой

– Load Balanced

Active-Passive

Избыточность — Redundancy

Холодный резерв

– Cold Standby

Тёплый резерв

– Warm Standby

Горячий резерв

– Hot Standby

С балансировкой

– Load Balanced

Active-Active

Избыточность — Redundancy



Холодный резерв

– Cold Standby

Тёплый резерв

– Warm Standby


Горячий резерв

– Hot Standby

С балансировкой

– Load Balanced


Избыточность — Redundancy



Холодный резерв	– Cold Standby
Тёплый резерв	– Warm Standby
Горячий резерв	– Hot Standby
С балансировкой	– Load Balanced

↑ Стоимость / Сложность

Избыточность — Redundancy



Холодный резерв	– Cold Standby
Тёплый резерв	– Warm Standby
Горячий резерв	– Hot Standby
С балансировкой	– Load Balanced

↑ Стоимость / Сложность

↓ Время восстановления

Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Восстанавливаемость

Целостность данных

Доступность — Availability

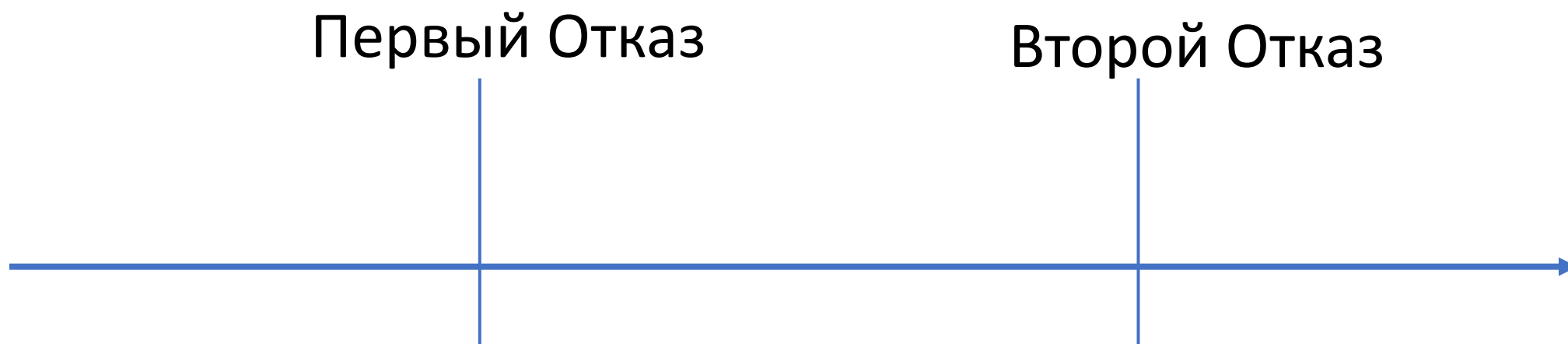


Доступность — Availability

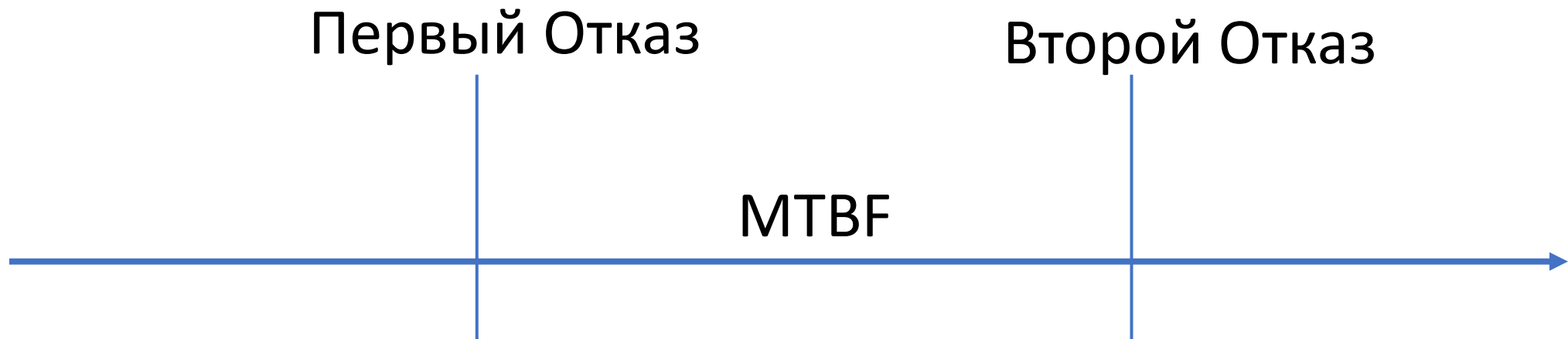
Первый Отказ



Доступность — Availability

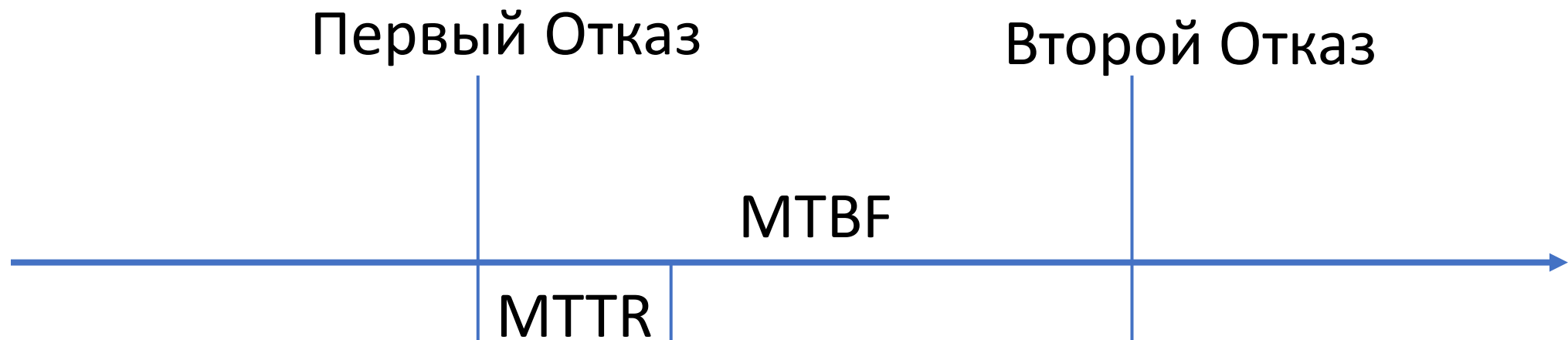


Доступность — Availability



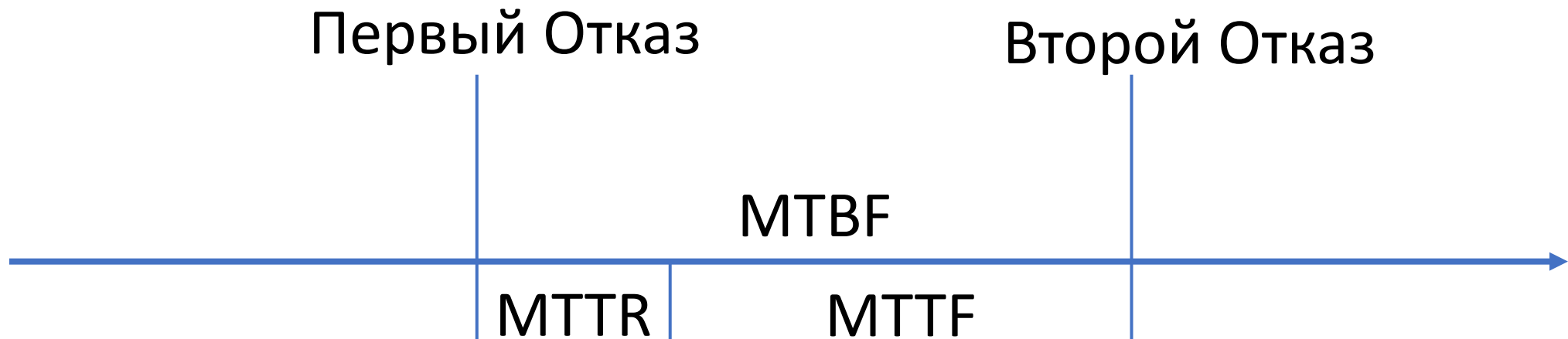
Mean Time Between Failures

Доступность — Availability



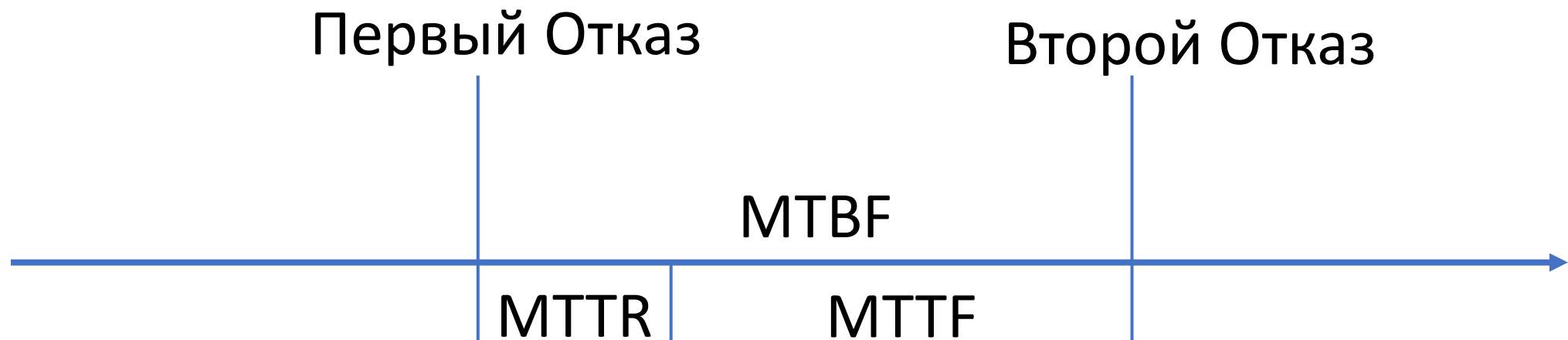
Mean Time To Recovery

Доступность — Availability



Mean Time To Failure

Доступность — Availability



$$\text{Availability} = \frac{\text{время работы (MTTF)}}{\text{всё время (MTBF)}}$$

Доступность — Availability

	%	В год	В месяц
1	90%	36.5 д	3 д
2	99%	3.5 д	7 ч
3	99.9%	9 ч	43 м
4	99.99%	50 м	4 м
5	99.999%	5 м	25 с
6	99.9999%	30 с	2.5 с
7	99.99999%	3 с	0.25 с

Доступность — Availability

	%	В год	В месяц
1	90%	36.5 д	3 д
2	99%	3.5 д	7 ч
3	99.9%	9 ч	43 м
4	99.99%	50 м	4 м
5	99.999%	5 м	25 с
6	99.9999%	30 с	2.5 с
7	99.99999%	3 с	0.25 с

Доступность — Availability



Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

Высокая доступность

Восстанавливаемость

Целостность данных

RPO и RTO



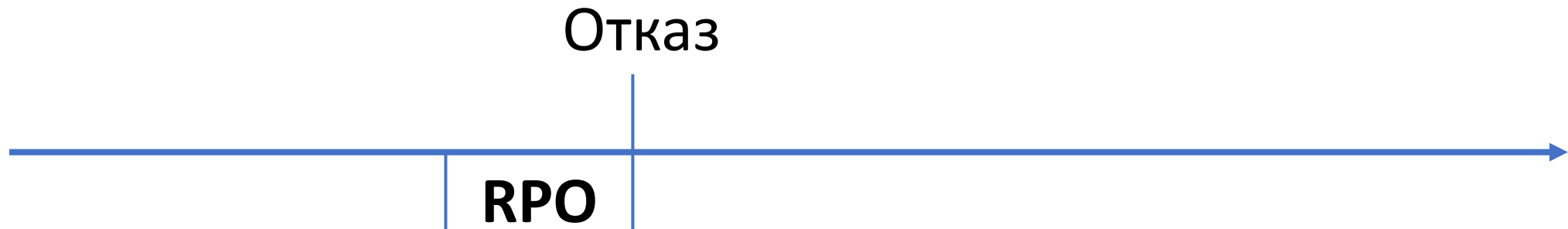
RPO и RTO

Отказ



RPO и RTO

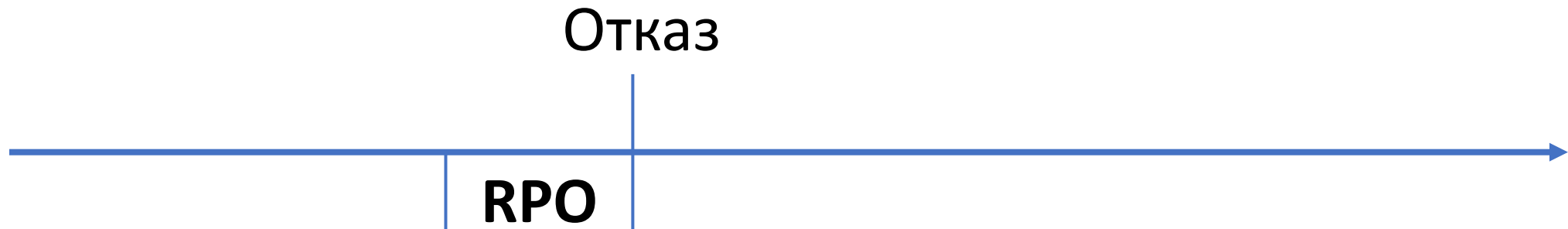
Recovery **Point** Objective



RPO и RTO

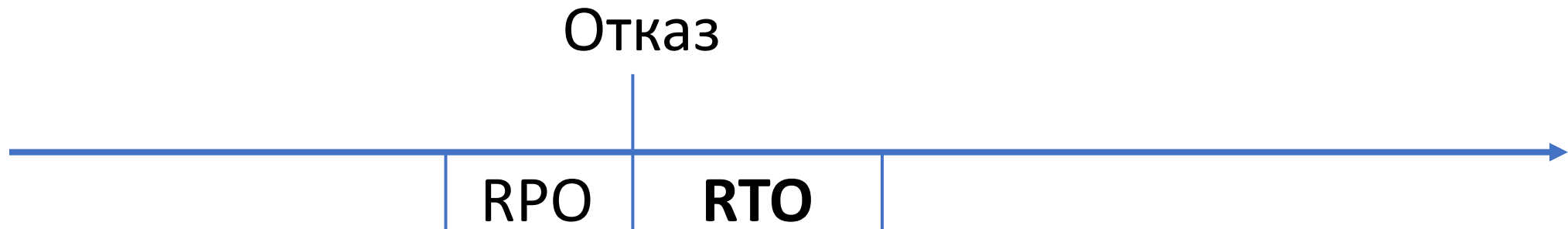
Recovery **Point** Objective

6 дней! (позже снизили до часов)



RPO и RTO

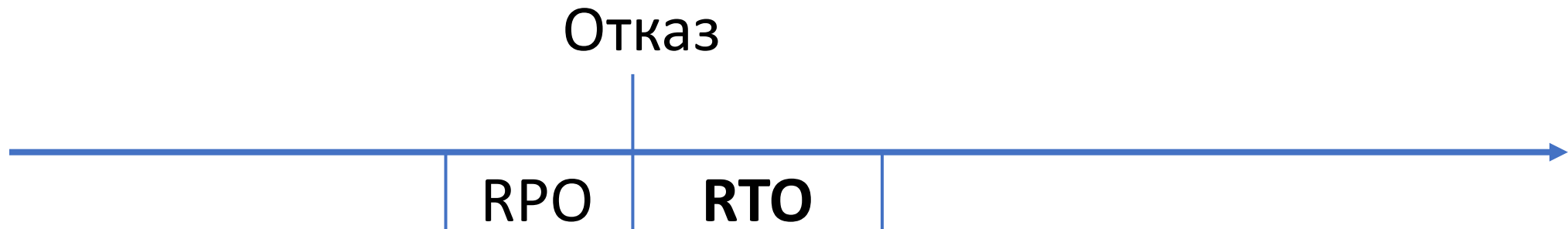
Recovery **Time** Objective



RPO и RTO

Recovery **Time** Objective

3 дня!



Надёжность

Устойчивость к высоким нагрузкам

Устойчивость к отказам

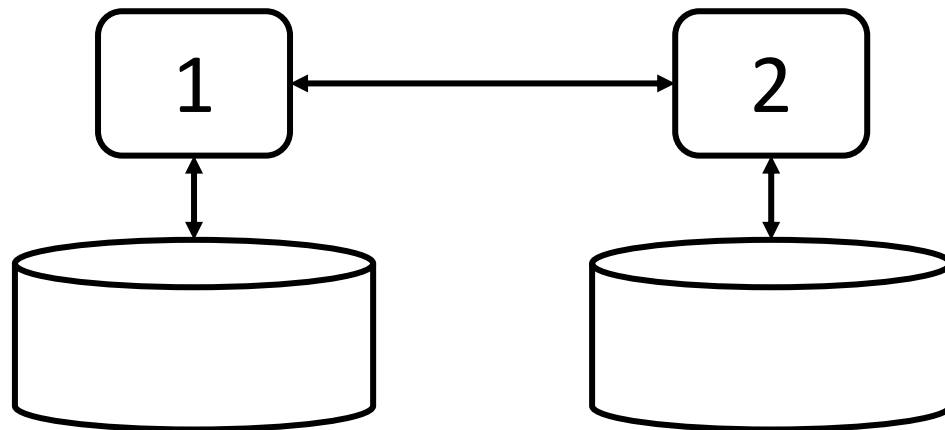
Высокая доступность

Восстанавливаемость

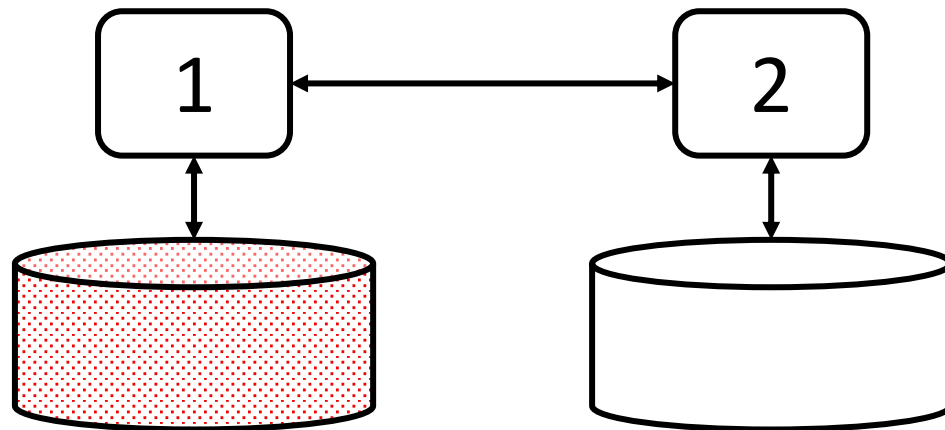
Целостность данных

Целостность данных

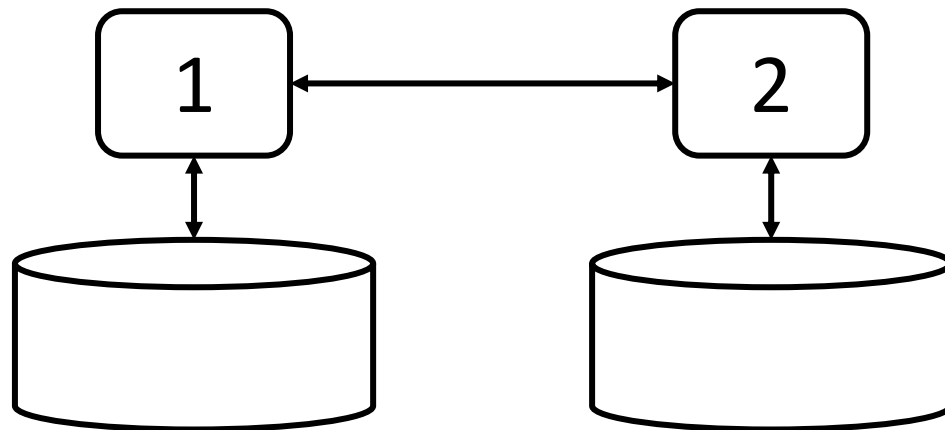
Целостность данных



Целостность данных



Целостность данных



Graceful Degradation

Изящная деградация

Деградация

Деградация

— По производительности

Деградация

- По производительности
- По функциональности

Деградация

- По производительности
- По функциональности
- По данным

Деградация

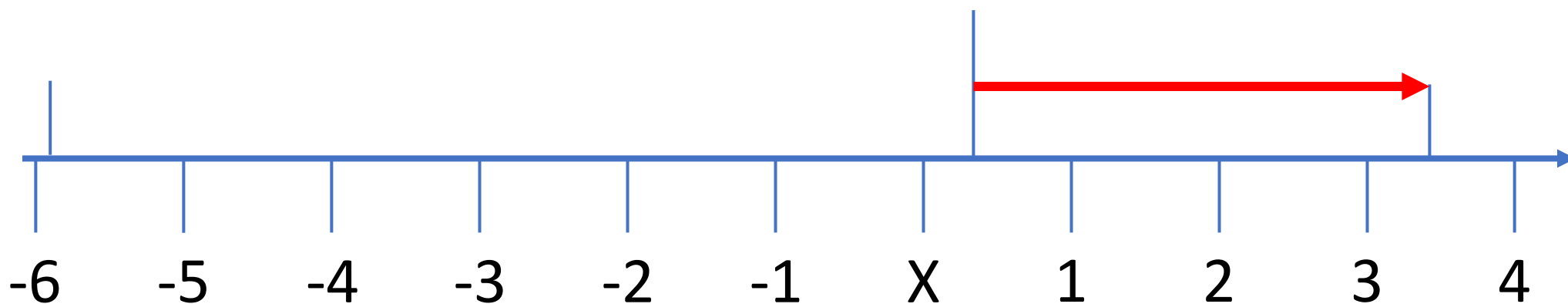
- По производительности
- По функциональности
- По данным
- По пользователям

Деградация

Как это было?

Деградация

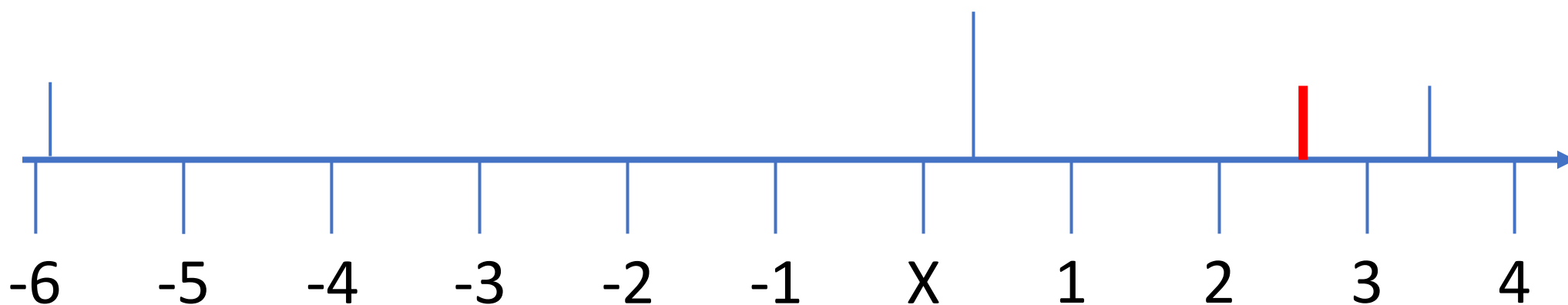
Как это было?



Деградация

Как это было?

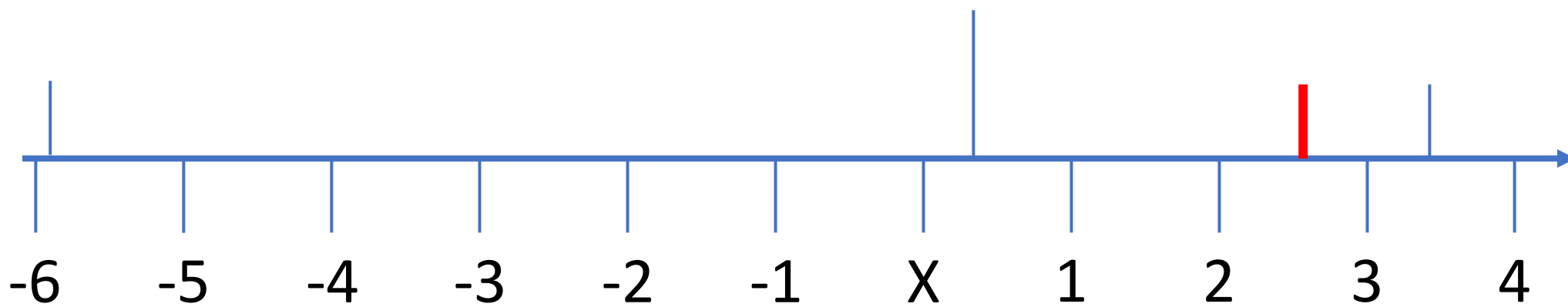
— На третьи сутки коротышки перешли на бересту



Деградация

Как это было?

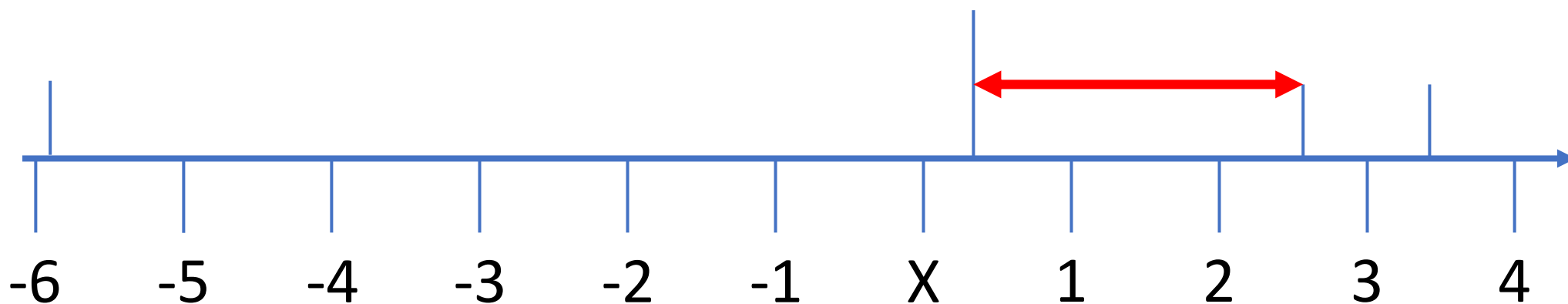
— На третьи сутки коротышки перешли на ^{бумагу}~~бересту~~



Деградация

Как это было?

- На третьи сутки коротышки перешли на ~~бересту~~ бумагу
- **Почему ждали 2 дня?**



Выводы

Выводы

SLA / SLO дают предсказуемость

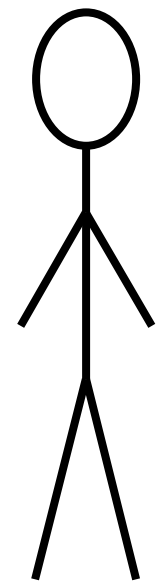
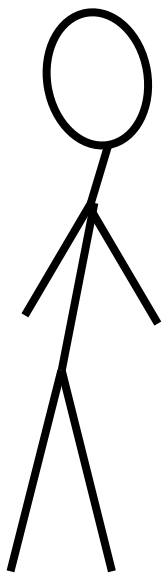
Выводы

SLA / SLO дают предсказуемость (риски!)

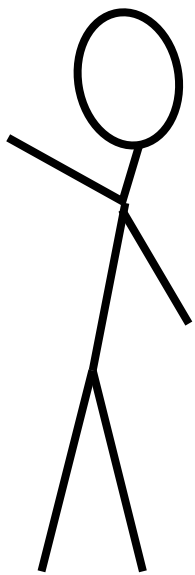
Выводы

SLA / SLO дают предсказуемость (риски!)

1. Проверь свои бэкапы
2. Посчитай метрики
3. Расскажи менеджерам о рисках



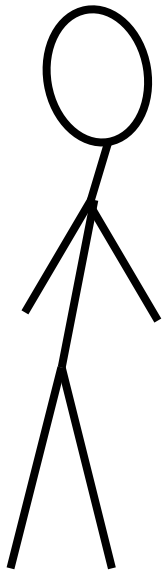
А В НАШЕМ СЕРВИСЕ
БУДЕТ ДОТУПНОСТЬ
5 ДЕВЯТОК!!!



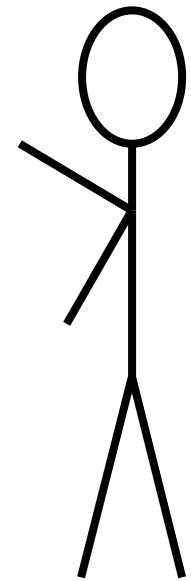
99.999% — это 5 минут в ГОД



А В НАШЕМ СЕРВИСЕ
БУДЕТ ДОТУПНОСТЬ
5 ДЕВЯТОК!!!

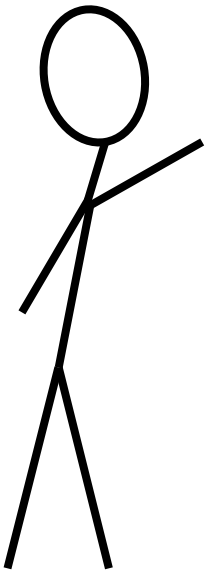


ДА?
А ТЫ ЗНАЕШЬ ДОСТУПНОСТЬ
СВОЕГО ДАТАЦЕНТРА?

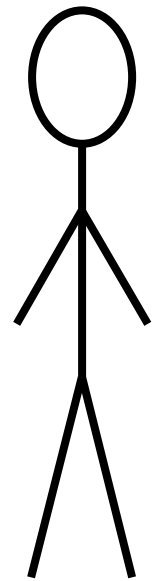


А В НАШЕМ СЕРВИСЕ
БУДЕТ ДОТУПНОСТЬ
5 ДЕВЯТОК!!!

Э-Э-Э...
НЕТ, НЕ ДУМАЮ...

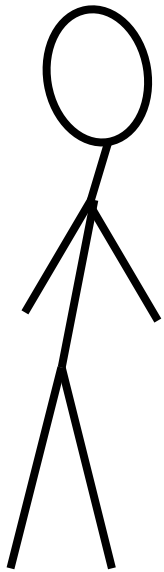


ДА?
А ТЫ ЗНАЕШЬ ДОСТУПНОСТЬ
СВОЕГО ДАТАЦЕНТРА?



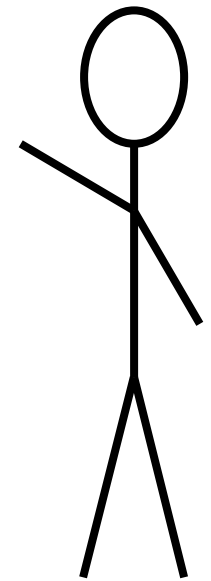
А В НАШЕМ СЕРВИСЕ
БУДЕТ ДОТУПНОСТЬ
5 ДЕВЯТОК!!!

Э-Э-Э...
НЕТ, НЕ ДУМАЮ...



ДА?
А ТЫ ЗНАЕШЬ ДОСТУПНОСТЬ
СВОЕГО ДАТАЦЕНТРА?

...99.95%

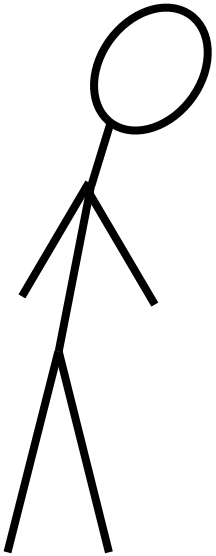


99.95% — это 20 минут в месяц

А В НАШЕМ СЕРВИСЕ
БУДЕТ ДОПУТНОСТЬ
5 ДЕВЯТОК!!!

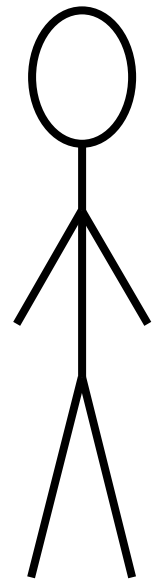
Э-Э-Э...
НЕТ, НЕ ДУМАЮ...

... НО... Я... МЫ...
ПРОЕКТИРОВАЛИ...



ДА?
А ТЫ ЗНАЕШЬ ДОСТУПНОСТЬ
СВОЕГО ДАТАЦЕНТРА?

...99.95%





 GregoryKoshelev

 chat_GregoryKoshelev

 gnkoshelev

tech.kontur.ru