Яндекс

Мониторинг XXI век

Алиса Смирнова,
Дима Никоненко,
Женя Бурнаев

Группа нагрузочного тестирования

Highload++, Москва, 25–26 октября 2010 года

Поговорим про мониторинги

План

1. Пороговый мониторинг vs Хороший
2. Оглянемся вокруг
3. Математические методы для мониторинга
4. Подробно рассмотрим повседневную задачу
5. Проведем аналогии
6. Общий подход к построению хорошего мониторинга
7. Примеры использования

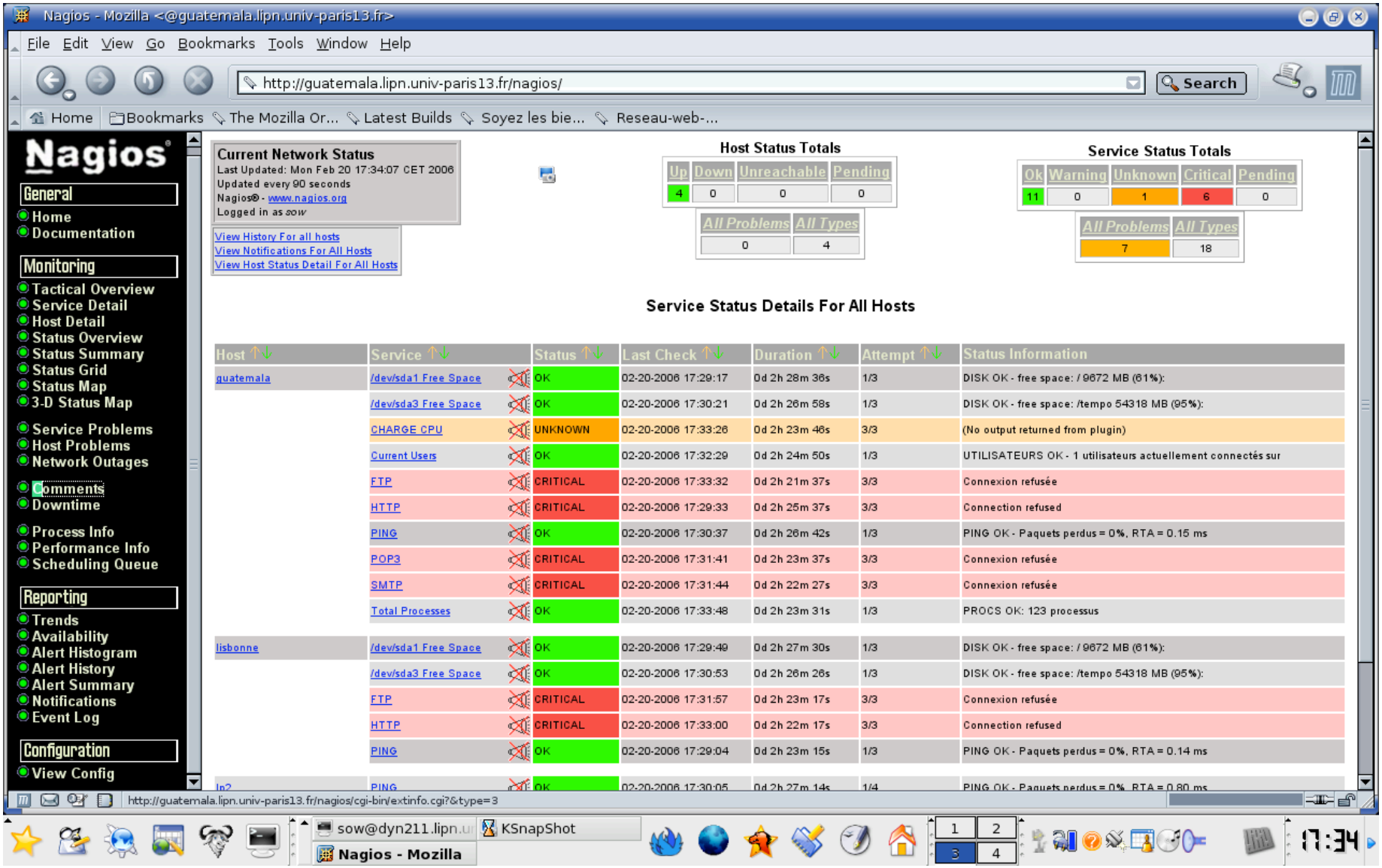
1. Пороговый мониторинг vs Хороший

2. Оглянемся вокруг

3. Математические методы для мониторинга

4. Рассмотрим повседневную задачу

Пороговый мониторинг


Nagios - Mozilla <@guatemala.lipn.univ-paris13.fr>
File Edit View Go Bookmarks Tools Window Help
http://guatemala.lipn.univ-paris13.fr/nagios/
Search
Home Bookmarks The Mozilla Or... Latest Builds Soyez les bie... Reseau-web-...
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Current Network Status
Last Updated: Mon Feb 20 17:34:07 CET 2006
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as sow
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Host Status Totals
Up Down Unreachable Pending
4 0 0 0
All Problems All Types
0 4
Service Status Totals
Ok Warning Unknown Critical Pending
11 0 1 6 0
All Problems All Types
7 18
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
guatemala /dev/sda1 Free Space OK 02-20-2006 17:29:17 0d 2h 28m 36s 1/3 DISK OK - free space: / 9672 MB (61%):
/dev/sda3 Free Space OK 02-20-2006 17:30:21 0d 2h 26m 58s 1/3 DISK OK - free space: /tempo 54318 MB (95%):
CHARGE CPU UNKNOWN 02-20-2006 17:33:26 0d 2h 23m 46s 3/3 (No output returned from plugin)
Current Users OK 02-20-2006 17:32:29 0d 2h 24m 50s 1/3 UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
FTP CRITICAL 02-20-2006 17:33:32 0d 2h 21m 37s 3/3 Connexion refusée
HTTP CRITICAL 02-20-2006 17:29:33 0d 2h 25m 37s 3/3 Connection refused
PING OK 02-20-2006 17:30:37 0d 2h 26m 42s 1/3 PING OK - Paquets perdus = 0%, RTA = 0.15 ms
POP3 CRITICAL 02-20-2006 17:31:41 0d 2h 23m 37s 3/3 Connexion refusée
SMTP CRITICAL 02-20-2006 17:31:44 0d 2h 22m 27s 3/3 Connexion refusée
Total Processes OK 02-20-2006 17:33:48 0d 2h 23m 31s 1/3 PROCS OK: 123 processus
lisbonne /dev/sda1 Free Space OK 02-20-2006 17:29:49 0d 2h 27m 30s 1/3 DISK OK - free space: / 9672 MB (61%):
/dev/sda3 Free Space OK 02-20-2006 17:30:53 0d 2h 26m 26s 1/3 DISK OK - free space: /tempo 54318 MB (95%):
FTP CRITICAL 02-20-2006 17:31:57 0d 2h 23m 17s 3/3 Connexion refusée
HTTP CRITICAL 02-20-2006 17:33:00 0d 2h 22m 17s 3/3 Connection refused
PING OK 02-20-2006 17:29:04 0d 2h 23m 15s 1/3 PING OK - Paquets perdus = 0%, RTA = 0.14 ms
ln2 PING OK 02-20-2006 17:30:05 0d 2h 27m 14s 1/4 PING OK - Paquets perdus = 0%, RTA = 0.80 ms
http://guatemala.lipn.univ-paris13.fr/nagios/cgi-bin/extinfo.cgi?&type=3
sow@dyn211.lipn.u
KSnapShot
Nagios - Mozilla
1 2 3 4
17:34

ZABBIX

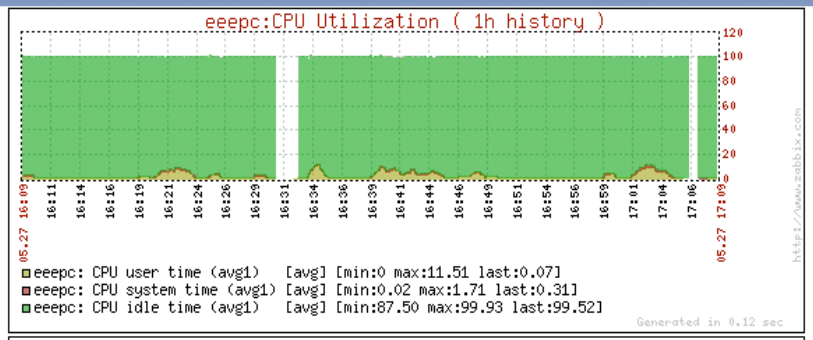
Help | Get support | Profile

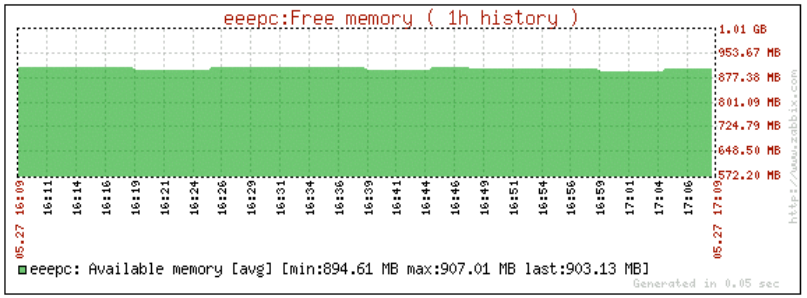
Monitoring | Inventory | Reports | Configuration | Administration | Login

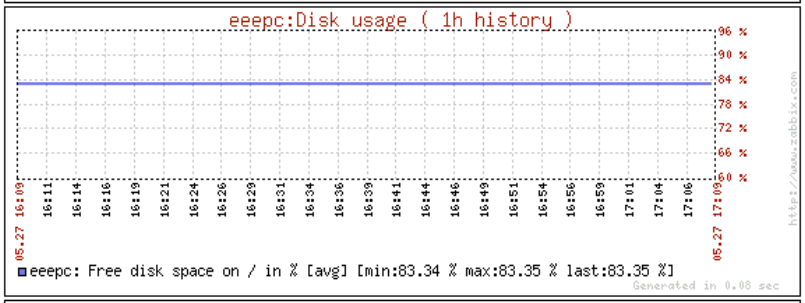
Overview | Web | Latest data | Triggers | Queue | Events | Actions | Maps | Graphs | Screens | Discovery | IT services

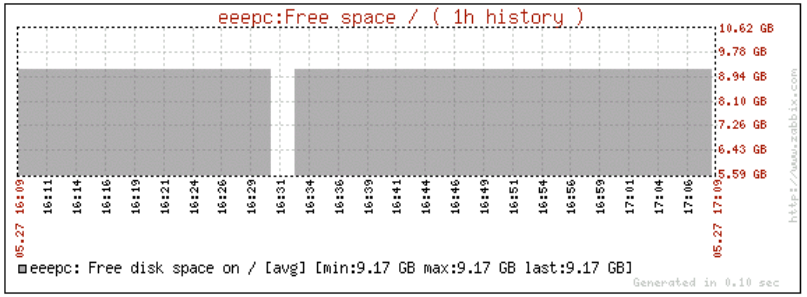
SCREENS / EeePC

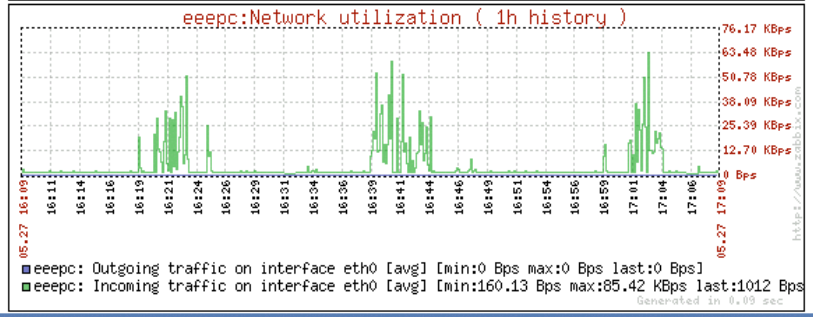
Screens: EeePC

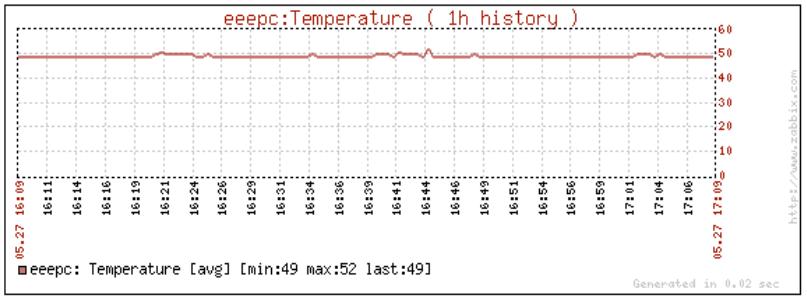








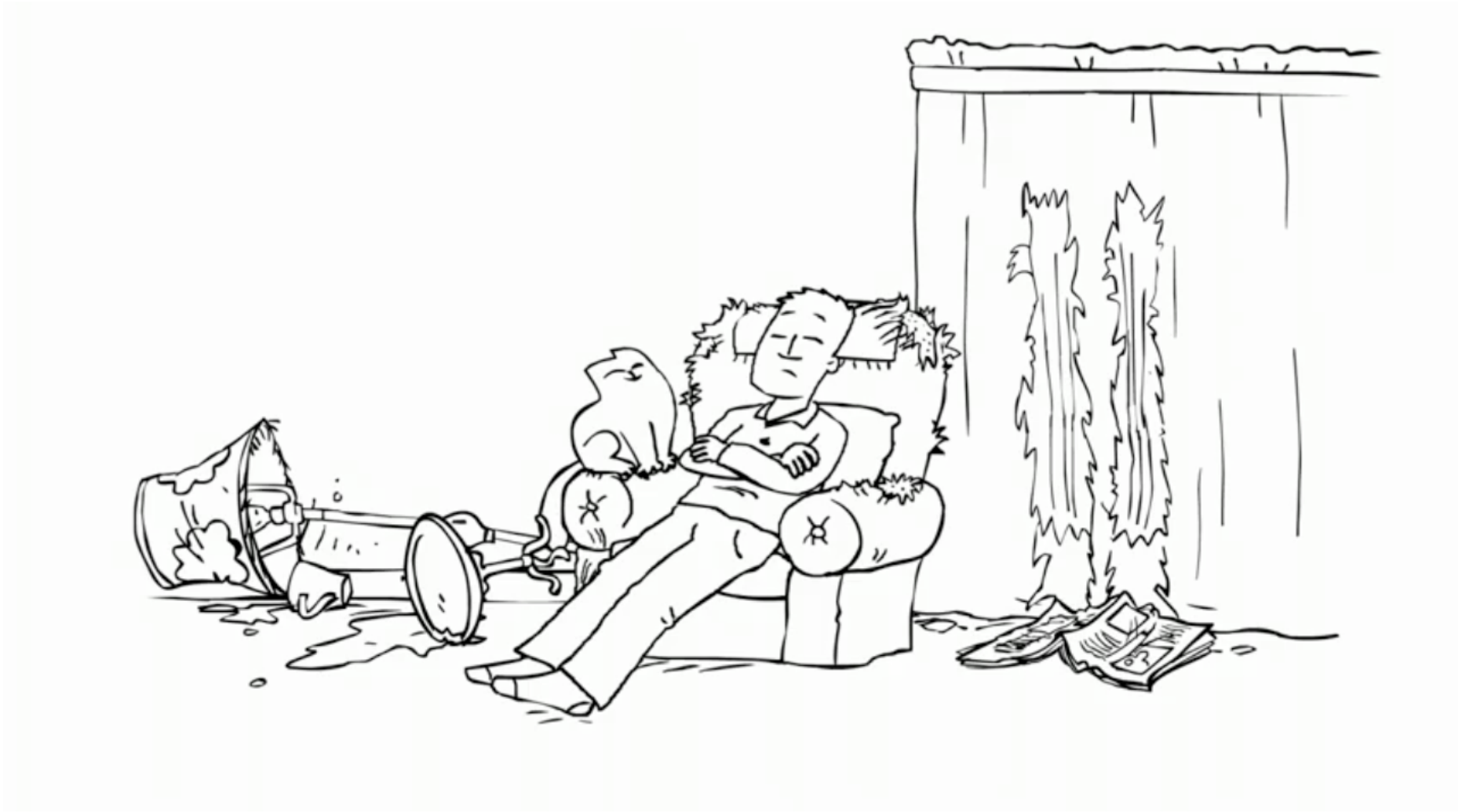




Navigate

Period: 1h | Decrease | Increase | Move: Left | Right | yyyymmddhhmm | go | reset

Звенит, когда уже все сломалось



Я

Хороший мониторинг

Звенит, когда еще не сломалось...

...но скоро сломается

Можно успеть принять меры

Пороговый мониторинг

Срабатывает при каждом пересечении

Я

Хороший мониторинг

Срабатывает один раз и по делу

Нет ложных тревог!

Я

Как найти хороший мониторинг?

1. Пороговый мониторинг vs Хороший

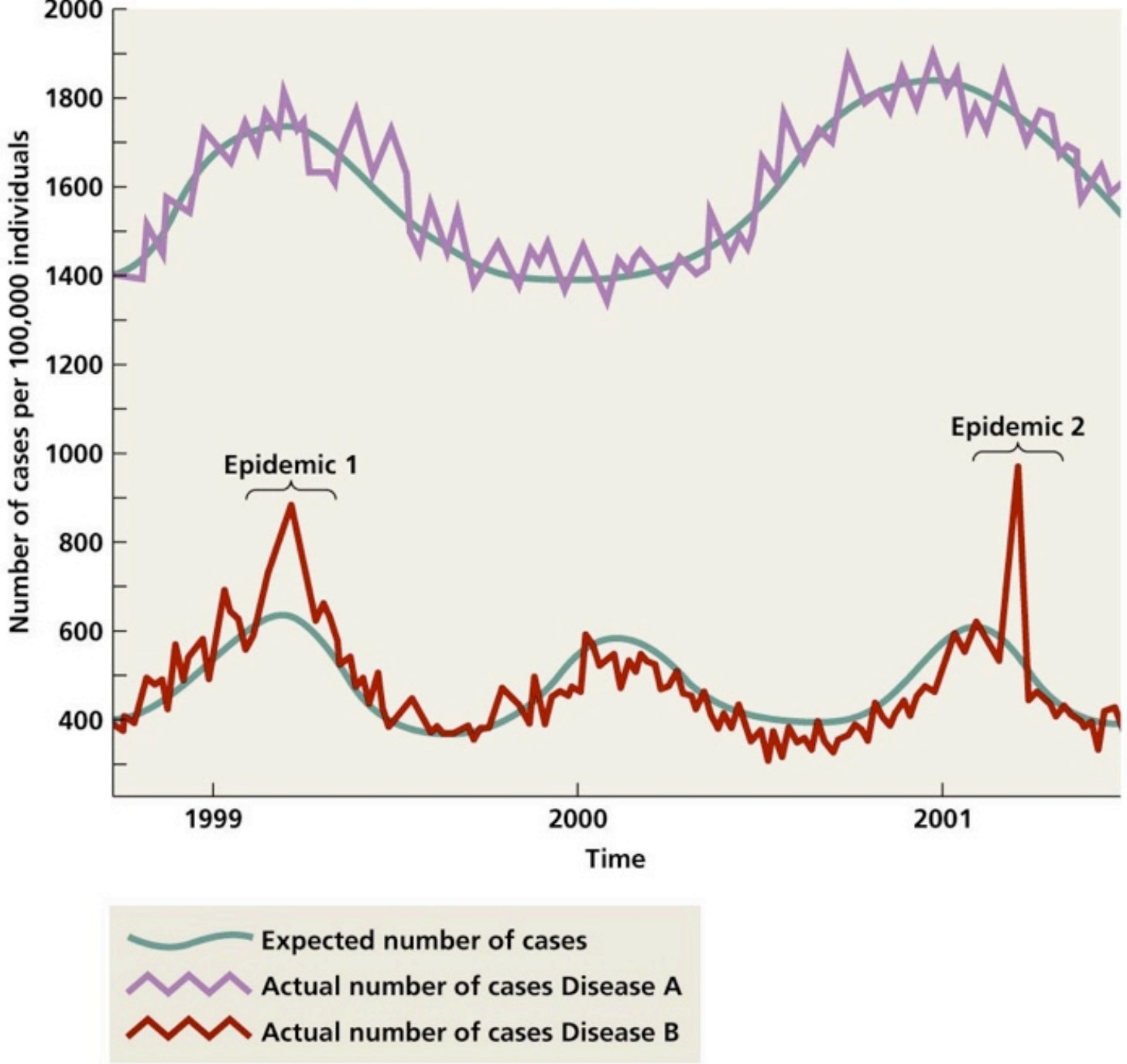
2. Оглянемся вокруг

3. Математические методы для мониторинга

4. Рассмотрим повседневную задачу

5. Проведем аналогии

В медицине - мониторинг эпидемий



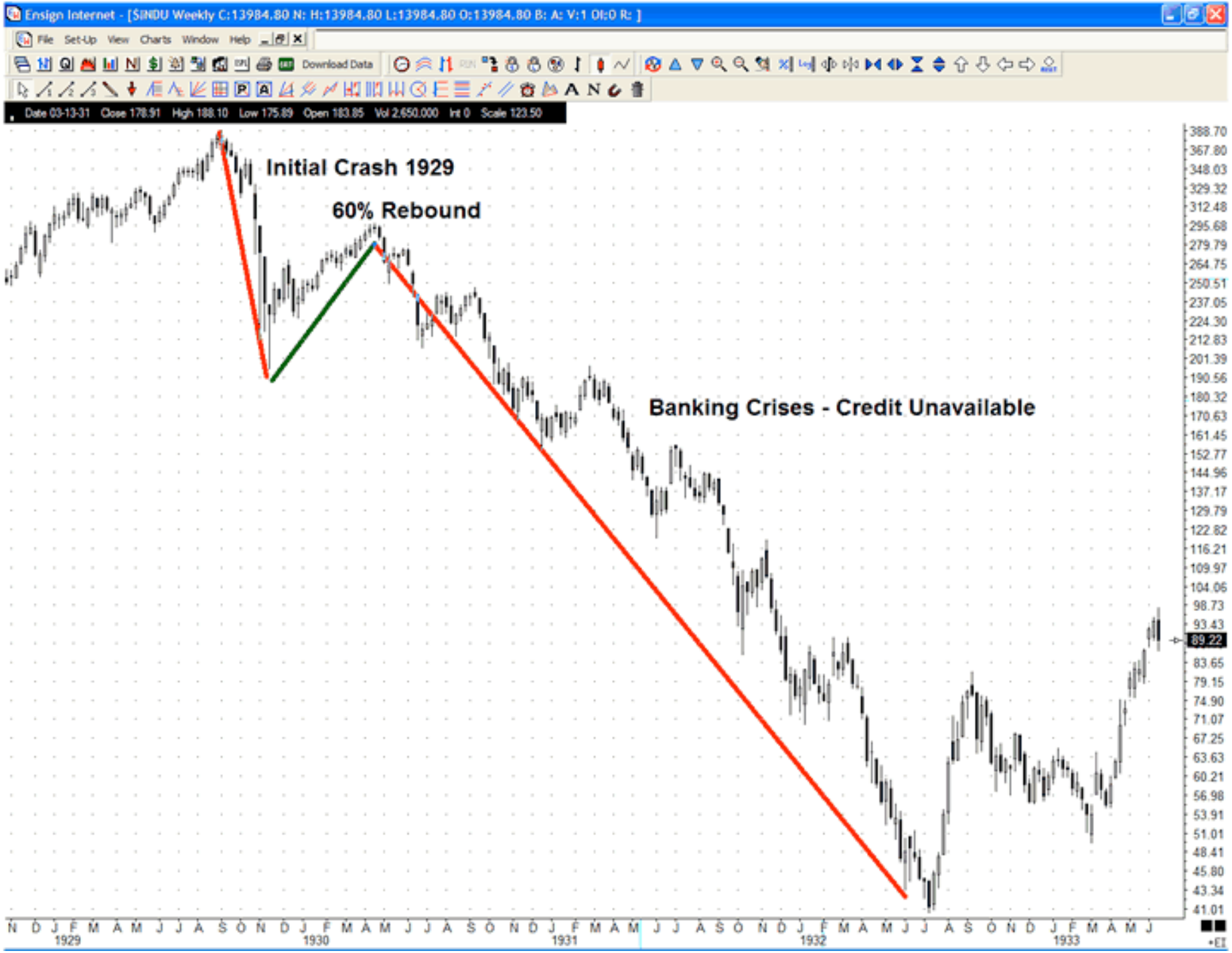
В навигации - мониторинг неисправностей датчиков

Я

В технике - мониторинг износа деталей

В экономике - мониторинг трендов

Я


Ensign Internet - [$INDU Weekly C:13984.80 N: H:13984.80 L:13984.80 O:13984.80 B: A: V:1 OI:0 R:]
File Set-Up View Charts Window Help
Download Data
Date 03-13-31 Close 178.91 High 188.10 Low 175.89 Open 183.85 Vol 2,650,000 Int 0 Scale 123.50
Initial Crash 1929
60% Rebound
Banking Crises - Credit Unavailable
388.70
367.80
348.03
329.32
312.48
295.68
279.79
264.75
250.51
237.05
224.30
212.83
201.39
190.56
180.32
170.63
161.45
152.77
144.96
137.17
129.79
122.82
116.21
109.97
104.06
98.73
93.43
89.22
83.65
79.15
74.90
71.07
67.25
63.63
60.21
56.98
53.91
51.01
48.41
45.80
43.34
41.01
N D J F M A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O N D J F M A M J
1929
1930
1931
1932
1933

А еще...

...мониторинг сейсмоактивности

Давным-давно...

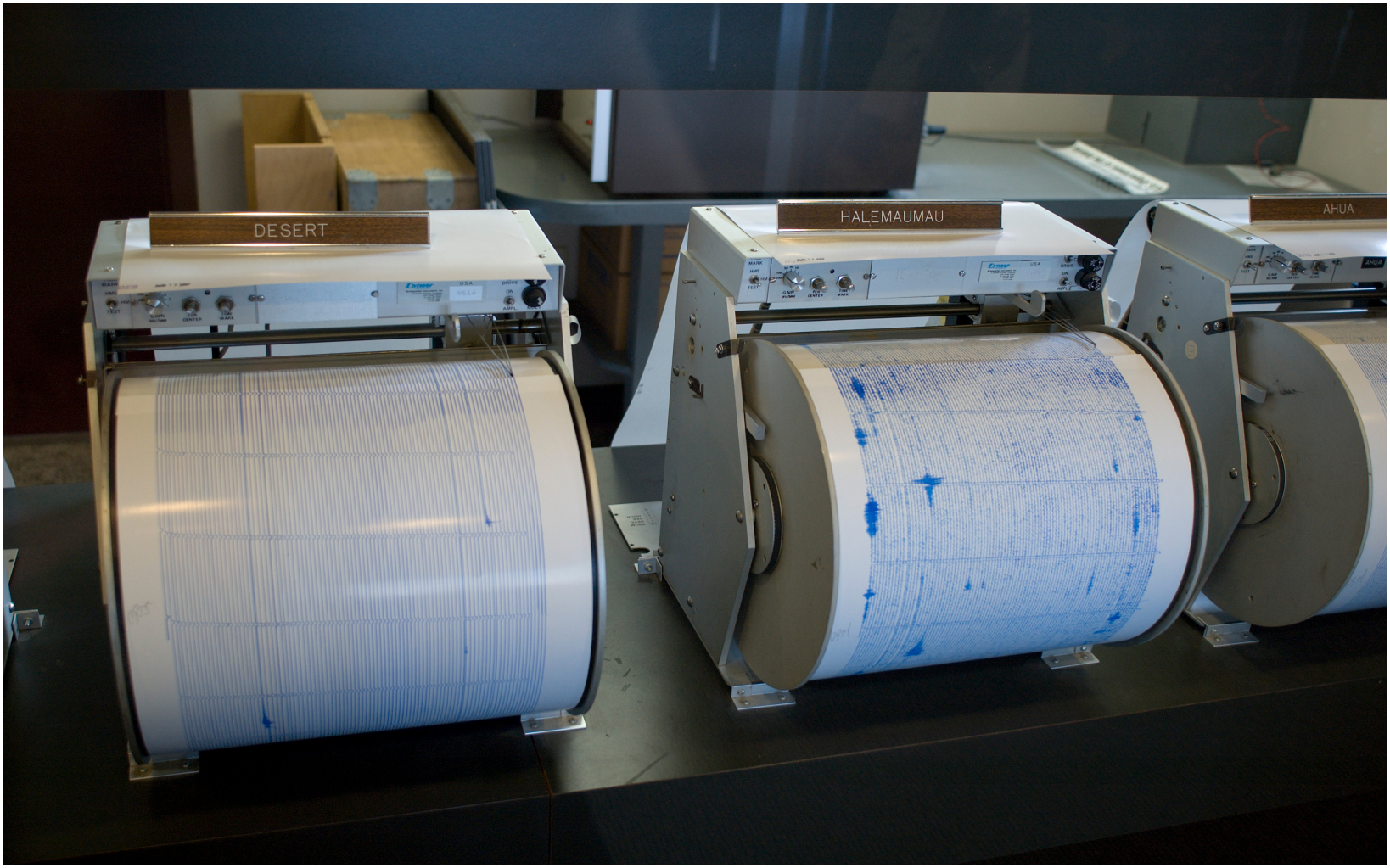
Я

Но сейчас...

Глобальная система...

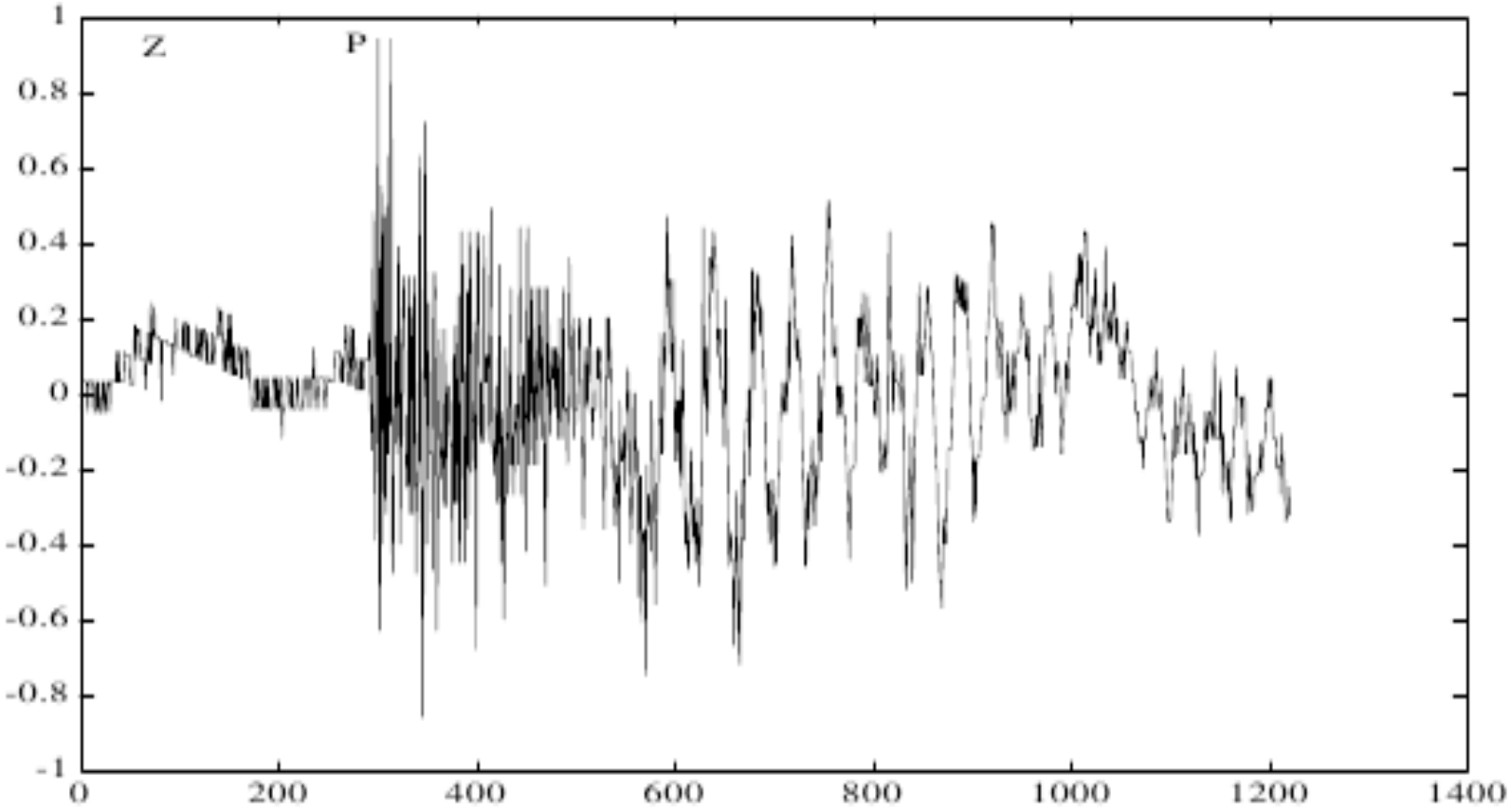
Я

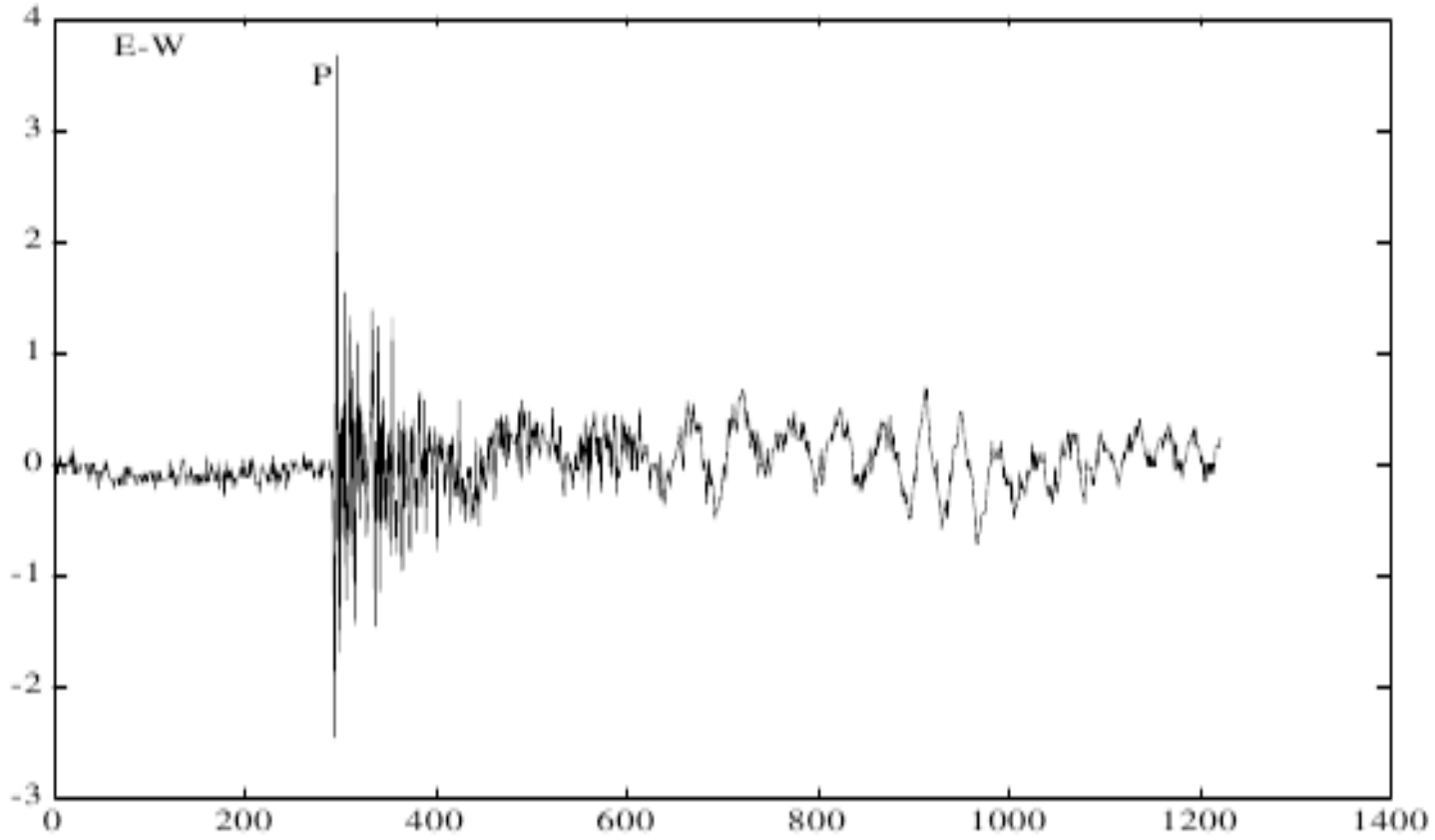
...из тысяч сейсмографов

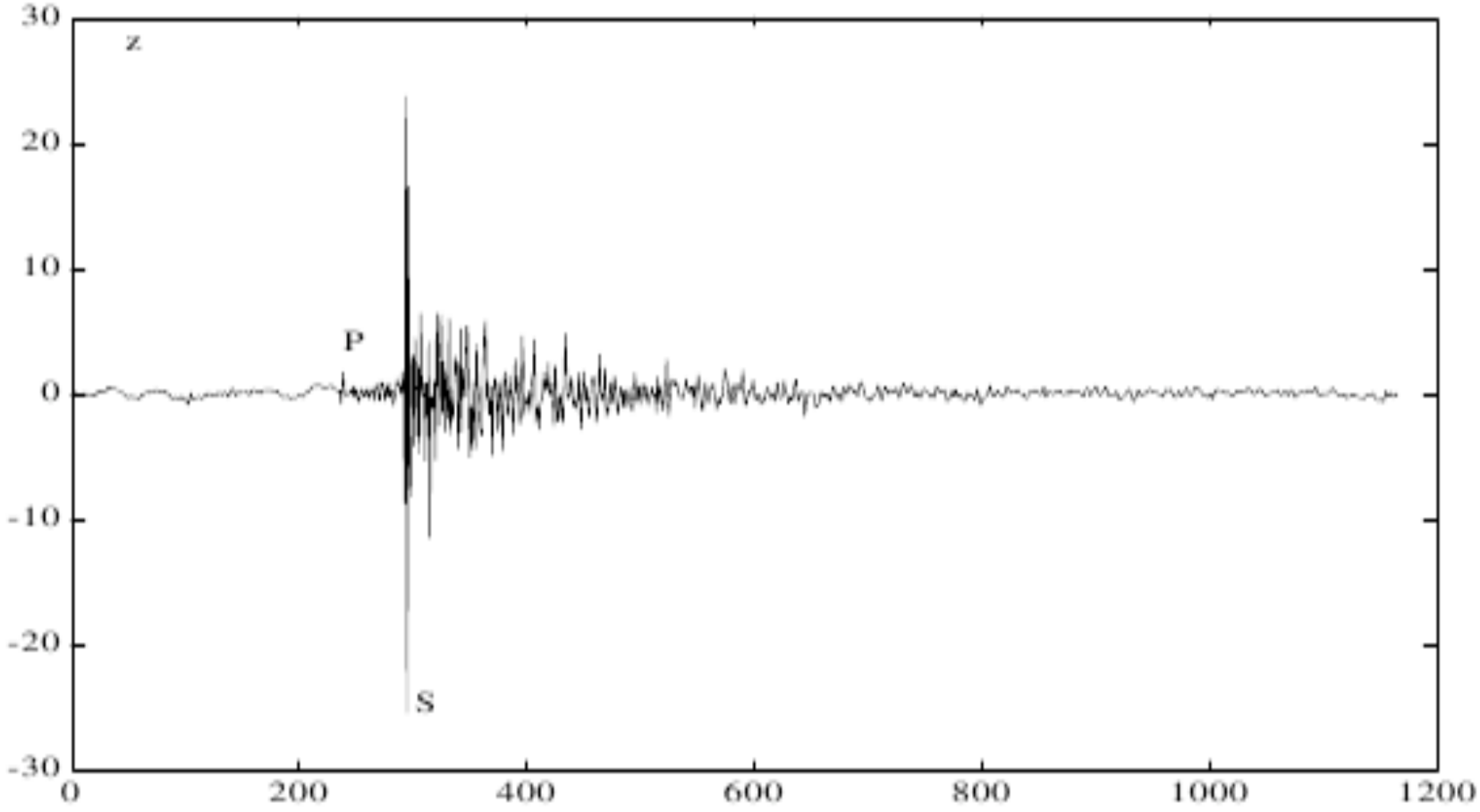


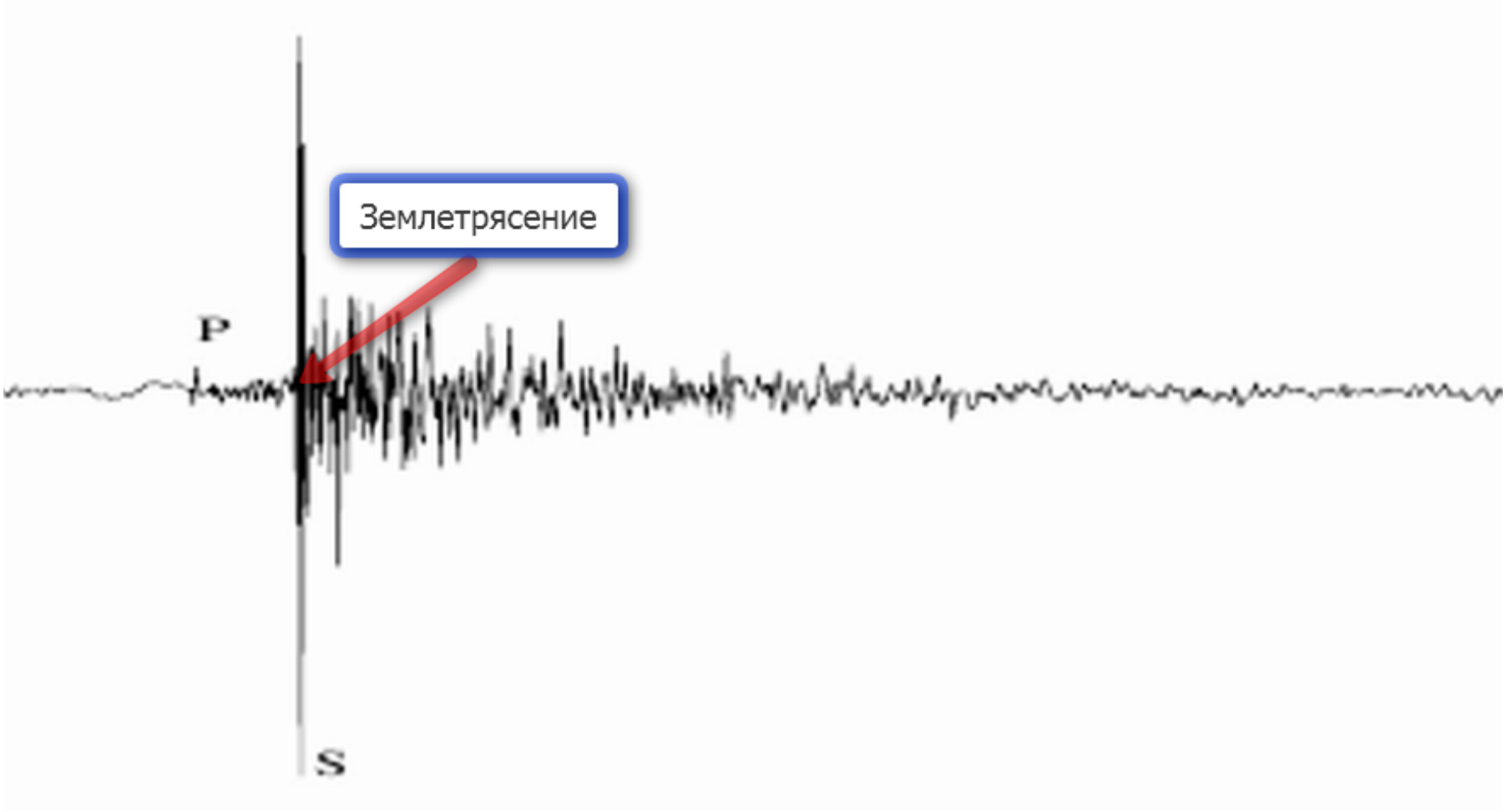
Я

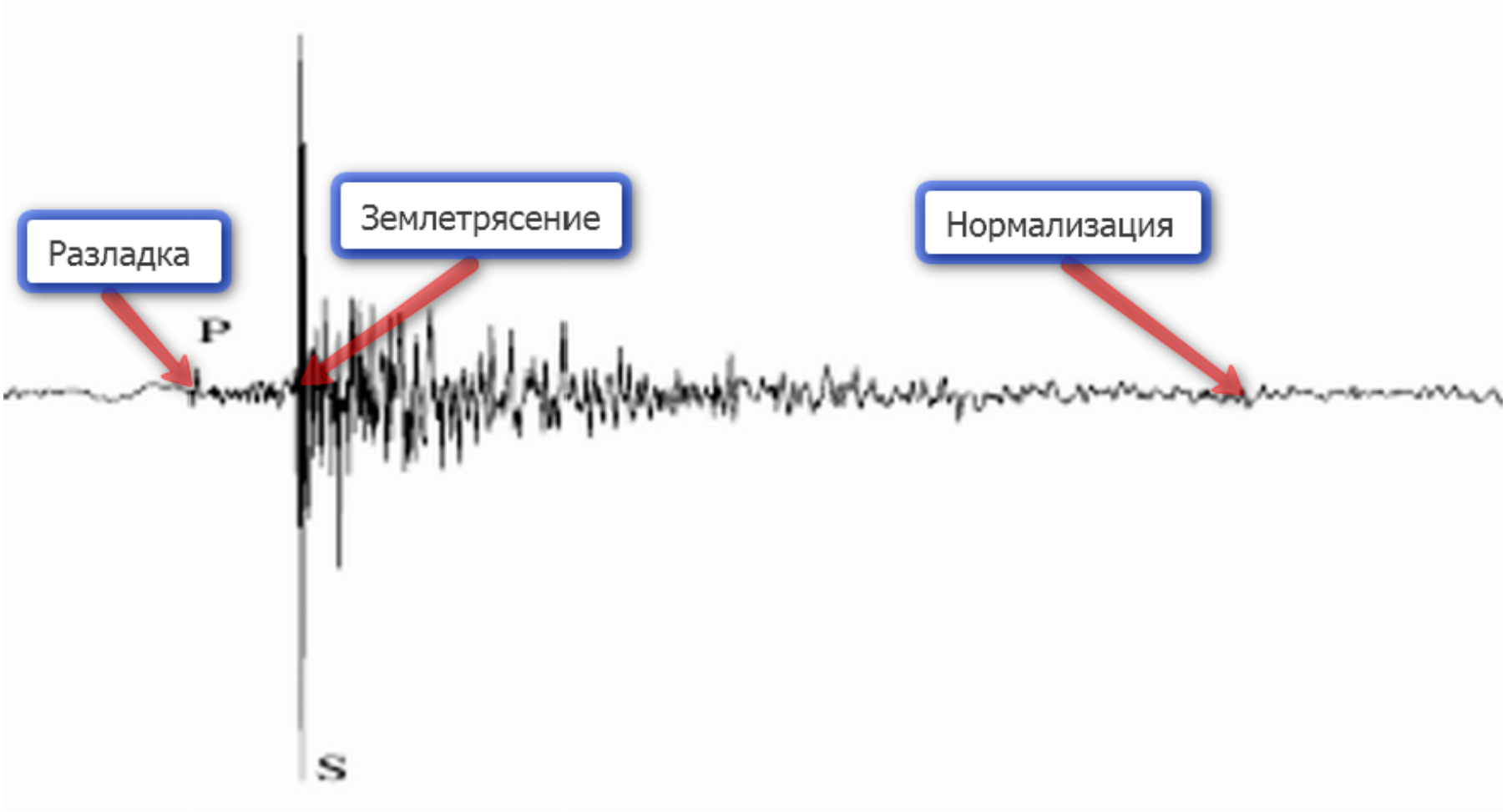
Сейсмоактивность — это случайный процесс


Z
P
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
0
200
400
600
800
1000
1200
1400


E-W
P
4
3
2
1
0
-1
-2
-3
0
200
400
600
800
1000
1200
1400


z
P
S
30
20
10
0
-10
-20
-30
0
200
400
600
800
1000
1200


Землетрясение
P
S


Разладка
Землетрясение
Нормализация
P
S

Нужен тонкий инструмент

Чтобы было просто

Данные

Система мониторинга

Сигнал тревоги

И надежно

Точность

Быстрота

В сейсмологии такая система уже есть

Я

В ее основе — умная математика полувековой выдержки

Я

1. Пороговый мониторинг vs Хороший
2. Оглянемся вокруг
3. Математические методы для мониторинга
4. Рассмотрим повседневную задачу
5. Проведем аналогии

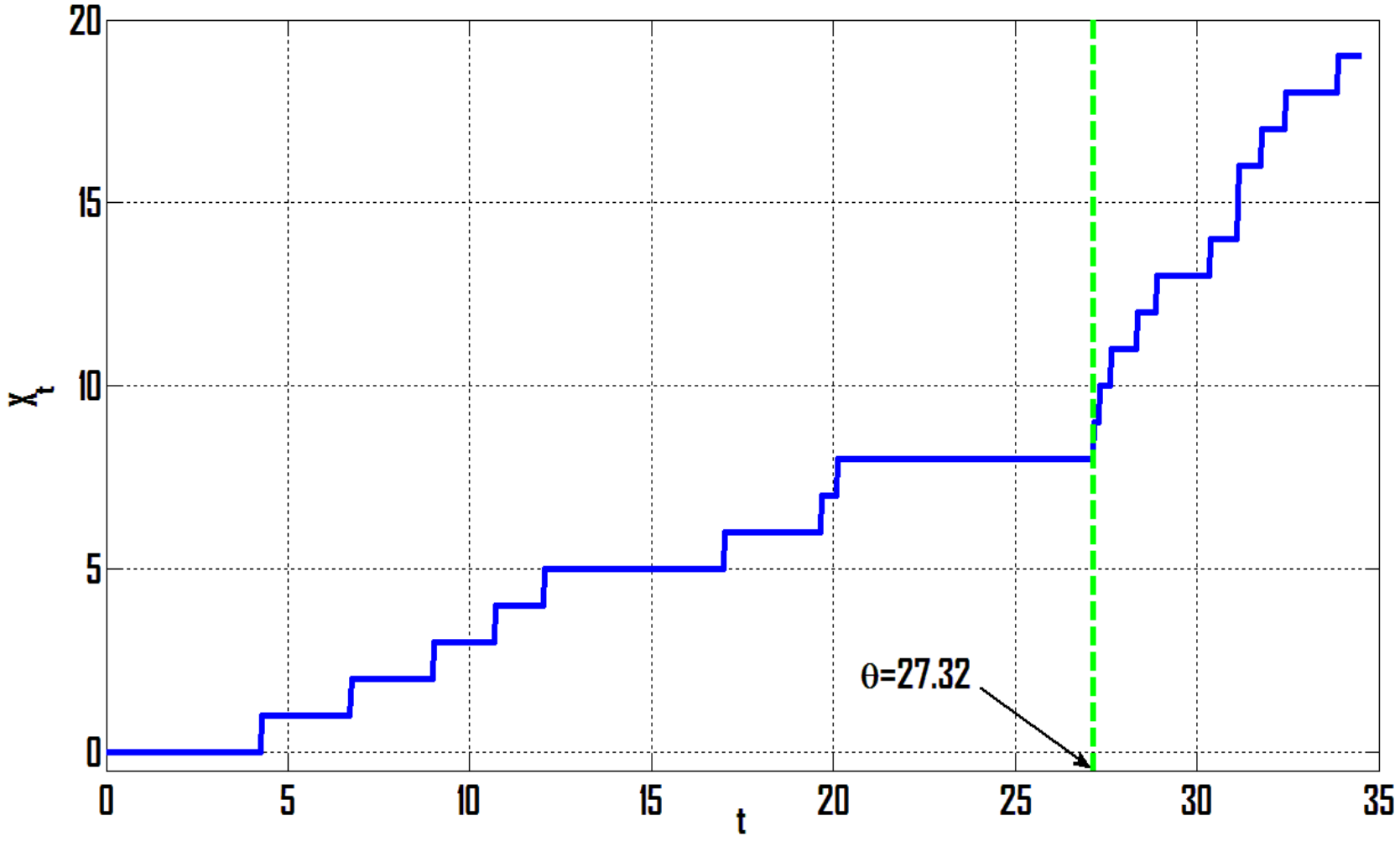
А подробнее

Существуют общие математические методы:

- Контрольные карты (Shewhart W.A., 1931);
- Метод кумулятивных сумм (Page E.S., 1954);
- Метод экспоненциально взвешенного скользящего среднего (Roberts S.W., 1959);
- Фильтр Калмана (Kalman R.E., 1960);
- Байесовские методы (Girshick M.A., Rubin H., 1952; Ширяев А.Н., 1961);
- Процедура Ширяева-Робертса (Ширяев А.Н., 1961; Roberts S.W., 1966);
- Метод на основе обобщенного отношения правдоподобия (Willsky A.S., 1976).

Из чего они возникли?

Пуассоновский процесс

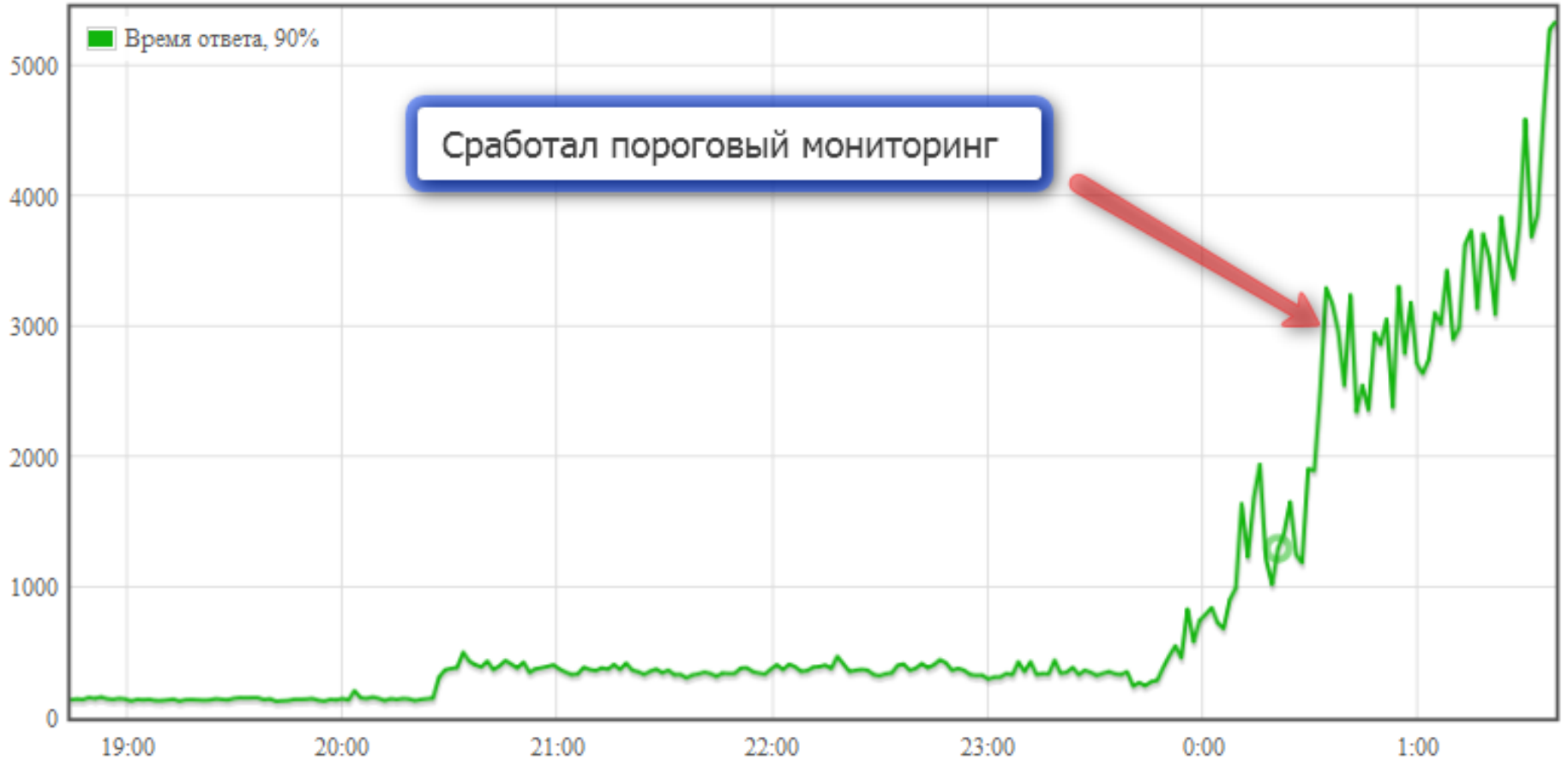


А решается она так:

Много формул.

1. Пороговый мониторинг vs Хороший
2. Оглянемся вокруг
3. Математические методы для мониторинга
4. Рассмотрим повседневную задачу
5. Проведем аналогии
6. Общий подход к построению хорошего мониторинга
7. Примеры использования

Пороговый мониторинг

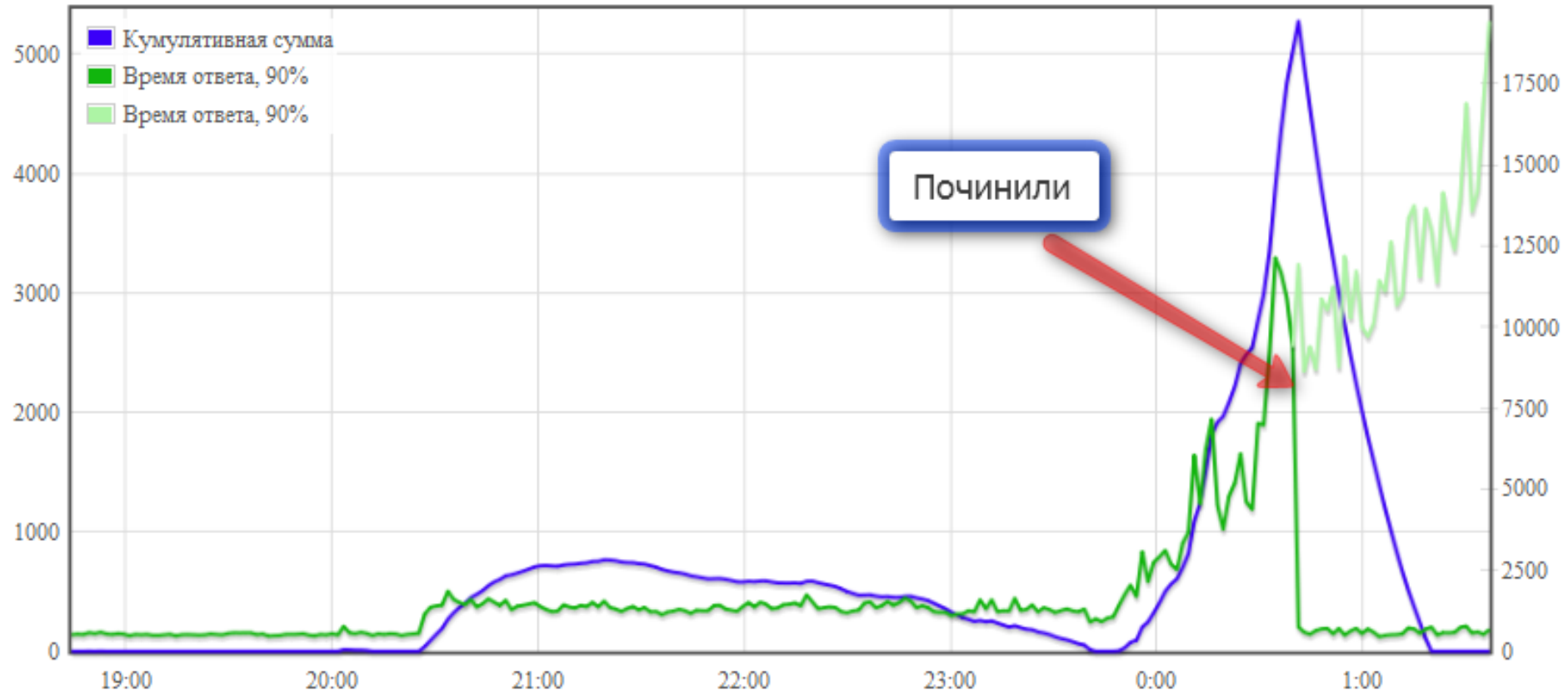


Я

Хороший мониторинг

Я

И стало вот так



Я

Как применить для мониторинга любого Интернет-сервиса?

2. Оглянемся вокруг

3. Математические методы для мониторинга

4. Рассмотрим повседневную задачу

5. Проведем аналогии

6. Общий подход к построению хорошего мониторинга

7. Примеры использования

Яндекс

Найдётся всё

Почта

логин

пароль

запомнить меня

Войти

вспомнить пароль

Завести почтовый ящик

Поиск Карты Маркет Новости Словари Блоги Видео

Например, the prodigy - omen

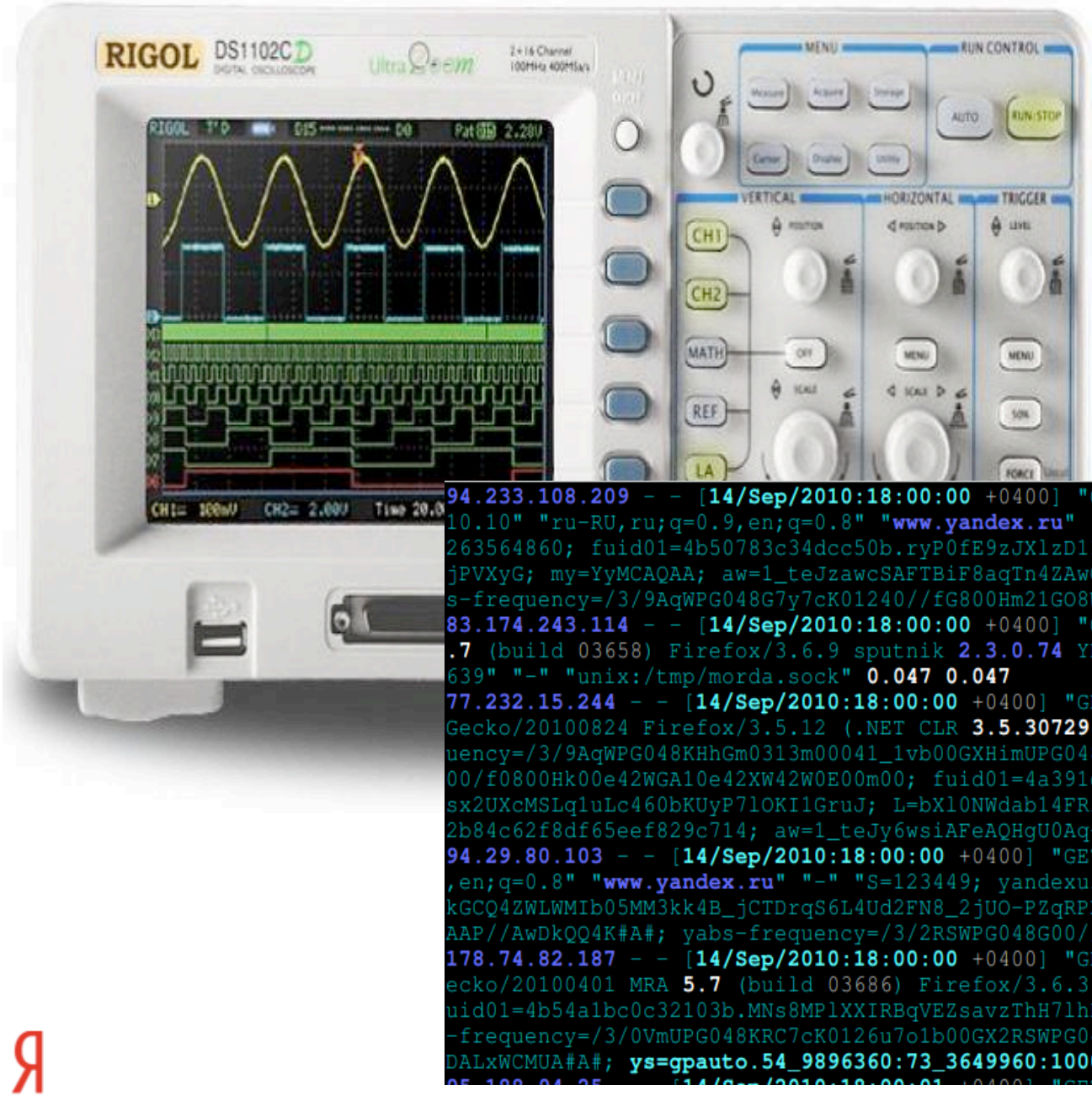
В Москве 17 октября, воскресенье, 21 23

Карта Москвы Схема метро Расписания Адреса и телефоны

Авто
рассчитайте стоимость

Маркет
обогреватели

Я




```
94.233.108.209 - - [14/Sep/2010:18:00:00 +0400] "GET / HTTP/1.1" 200 24506 "http
10.10" "ru-RU,ru;q=0.9,en;q=0.8" "www.yandex.ru" "-" "w=%2A1..c41y3O..1278700336
263564860; fuid01=4b50783c34dcc50b.ryP0fE9zJXlzD11xHcZzdaGxPGTWc102ISdJUB9ol4CqA
jPVXyG; my=YyMCAQAA; aw=1_teJzawcSAFTBiF8aqTn4ZAwOvMgPD11BidY0CZMDCAAk/Lm1IWMLAN
s-frequency=/3/9AqWPG048G7y7cK01240//fG800Hm21GO8W0K71GW910GG0mO30WO22G83WG420GK
83.174.243.114 - - [14/Sep/2010:18:00:00 +0400] "GET / HTTP/1.1" 200 25268 "-" "
.7 (build 03658) Firefox/3.6.9 sputnik 2.3.0.74 YB/5.0.3" "ru-ru,ru;q=0.8,en-us;
639" "-" "unix:/tmp/morda.sock" 0.047 0.047
77.232.15.244 - - [14/Sep/2010:18:00:00 +0400] "GET / HTTP/1.1" 200 24996 "http:
Gecko/20100824 Firefox/3.5.12 (.NET CLR 3.5.30729) YB/4.3.0" "ru-ru,ru;q=0.8,en-
uency=/3/9AqWPG048KHhGm0313m00041_1vb00GXHimUPG048KsM66K312S0005Hx1zb00GX2RSWPG0
00/f0800Hk00e42WGA10e42XW42W0E00m00; fuid01=4a391d3807a09dcc.GGpH-VlAaAudKkeX3OQ
sx2UXcMSLq1uLc460bKUyP7lOKI1GruJ; L=bXl0NWdab14FRlV2RmdQdFoAcgFeUX90TjEIFSwrGQAd
2b84c62f8df65eef829c714; aw=1_teJy6wsiAFeAQHgU0Aq+VGBjuajIwLF2CENsawAiPh79vk32IN
94.29.80.103 - - [14/Sep/2010:18:00:00 +0400] "GET / HTTP/1.1" 200 24113 "-" "Op
,en;q=0.8" "www.yandex.ru" "-" "S=123449; yandexuid=9142121491267616869; fuid01=
kGCQ4ZWLWMIb05MM3kk4B_jCTDrqS6L4Ud2FN8_2jUO-PZqRPXpT_8fN8r-97n2kDCd5; aw=1_teJy6
AAP//AwDkQQ4K#A#; yabs-frequency=/3/2RSWPG048G00//fG800G41" "-" "unix:/tmp/morda
178.74.82.187 - - [14/Sep/2010:18:00:00 +0400] "GET / HTTP/1.1" 200 24772 "http:
ecko/20100401 MRA 5.7 (build 03686) Firefox/3.6.3 ( .NET CLR 3.5.30729) sputnik
uid01=4b54a1bc0c32103b.MNs8MPlXXIRBqVEZsavzThH7lhHRjjqUMH1Kgl2mfqz2DQKvDLfDH3ml5
-frequency=/3/0VmUPG048KRC7cK0126u7o1b00GX2RSWPG048G00//fG800GO42maF30i0; aw=1_t
DALxWCMUA#A#; ys=gpauto.54_9896360:73_3649960:100000.0000000:1:1284483586; t=p"
```


twitter
Home ›
Twitter is over capacity.
Please wait a moment and try again. For more information, check out Twitter Status »
© 2010 Twitter
About Us
Contact
Blog
Status
API
Help
Jobs
TOS
Privacy

Современные методы

- Асимптотически оптимальные методы (на основе обобщенного отношения правдоподобия) выявления разладки в случае нескольких каналов наблюдений (Никифоров 2000, 2003; Тартаковский, Розовский 2006, 2008).
- Оптимальные методы обнаружения разладки для случая платы за получение новых наблюдений (Ширяев, 2010)
- Методы обнаружения разладки для процессов со скачками (Пешкир, Ширяев, 2000).
- Методы обнаружения разладки для диффузионных процессов (Гапеев, Ширяев, 2009)

Я

От теории — к практике

3. Математические методы для мониторинга

4. Рассмотрим повседневную задачу

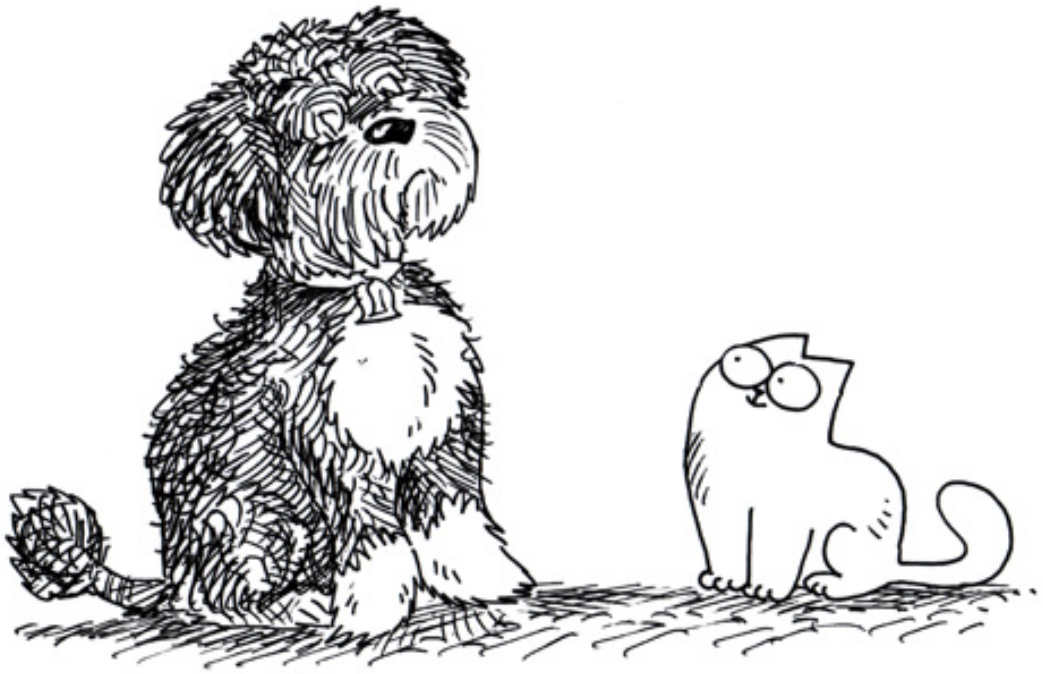
5. Проведем аналогии

6. Общий подход к построению хорошего мониторинга

7. Примеры

Все сервисы разные

Постановка задачи



Я

Что мониторить?

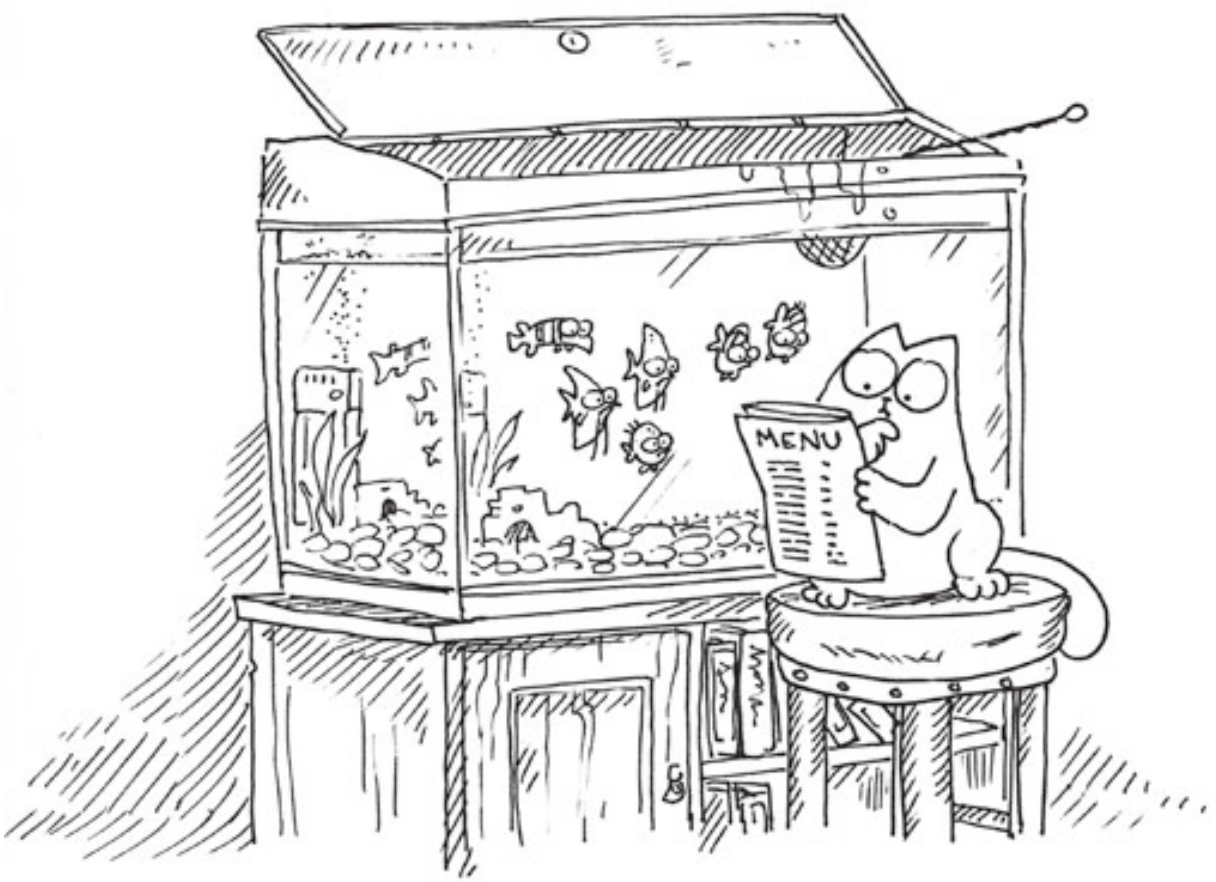
Что считать разладкой?

Какой должна быть

— Точность обнаружения

— Вероятность ложного срабатывания

Сбор данных

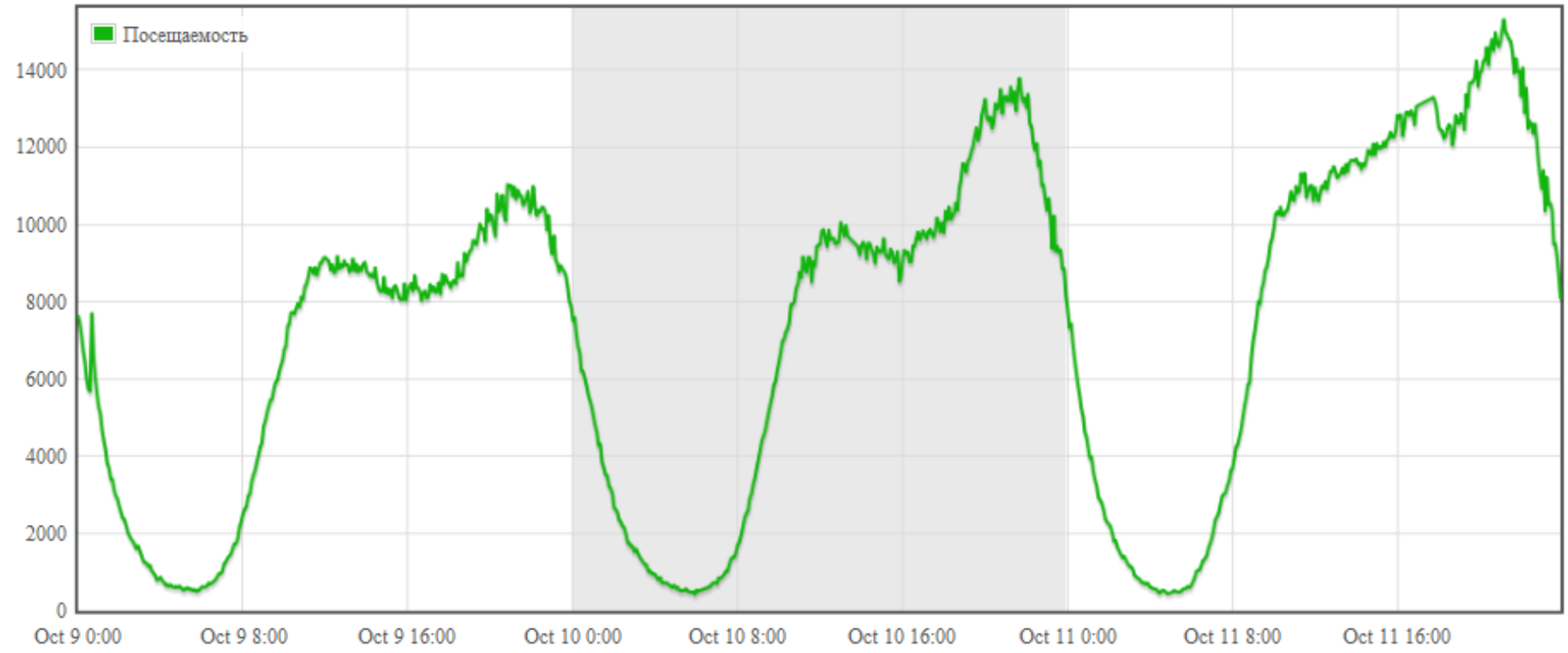


Я

Предобработка…

...слияние данных из разных источников

...выделение циклов


Посещаемость
14000
12000
10000
8000
6000
4000
2000
0
Oct 9 0:00
Oct 9 8:00
Oct 9 16:00
Oct 10 0:00
Oct 10 8:00
Oct 10 16:00
Oct 11 0:00
Oct 11 8:00
Oct 11 16:00

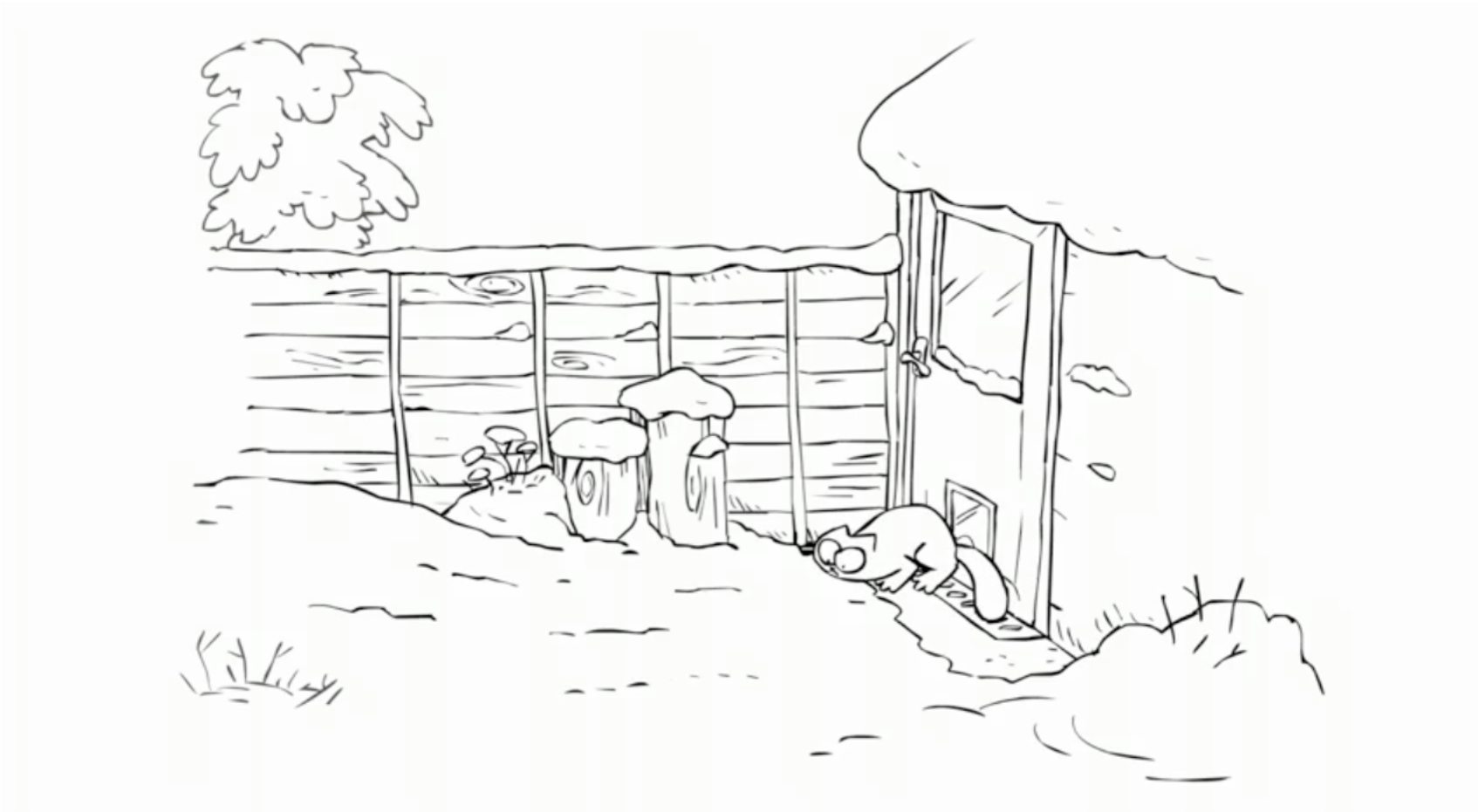
Я

...нормировка


Посещаемость
1.3
1.2
1.1
1.0
0.9
0.8
0.7
0.6
0.5
Oct 9 0:00
Oct 9 8:00
Oct 9 16:00
Oct 10 0:00
Oct 10 8:00
Oct 10 16:00
Oct 11 0:00
Oct 11 8:00
Oct 11 16:00

Я

Эксперименты



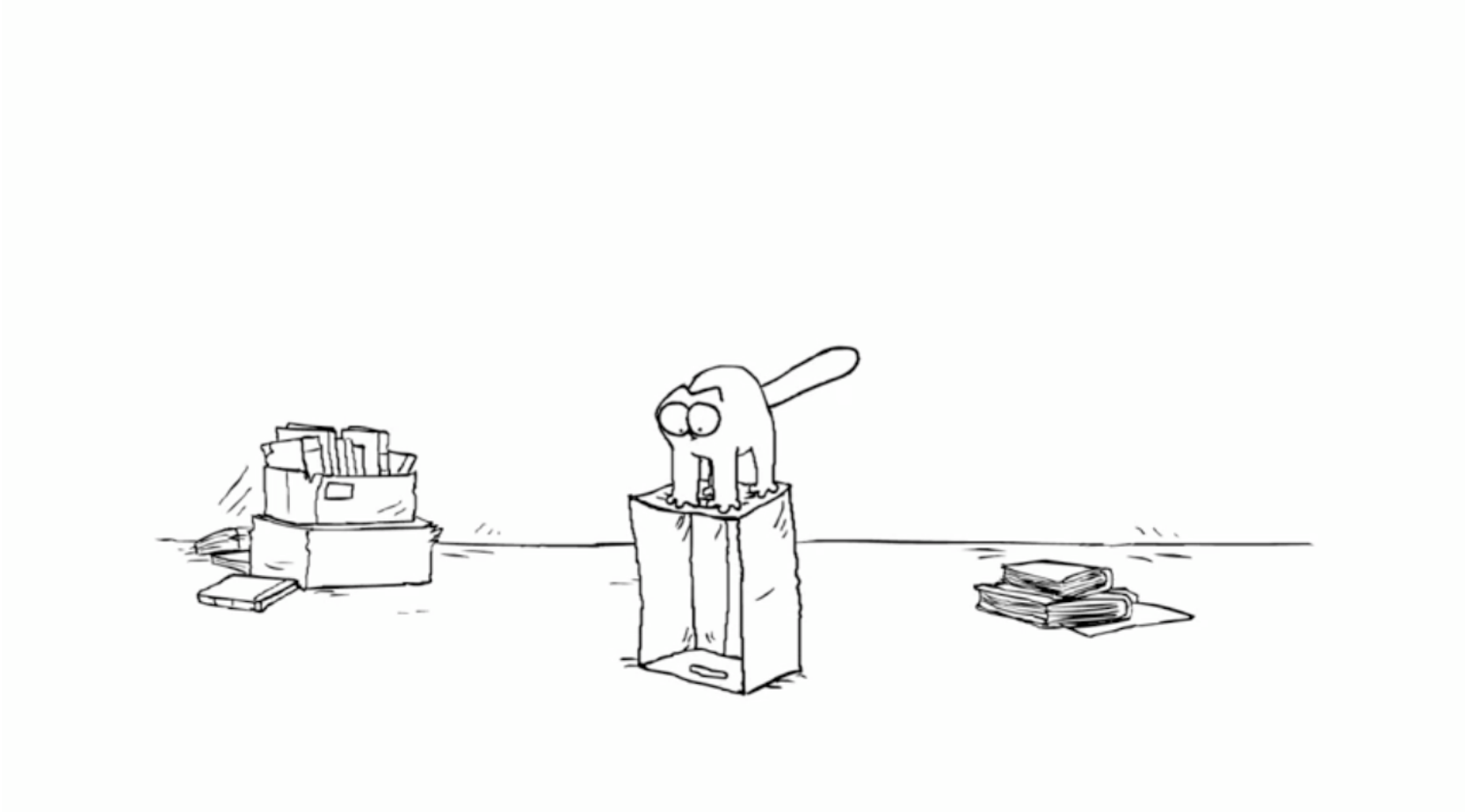
Я

Подбор параметров

Настройка сигналов о разладке

Автоматизация

Оценка результата



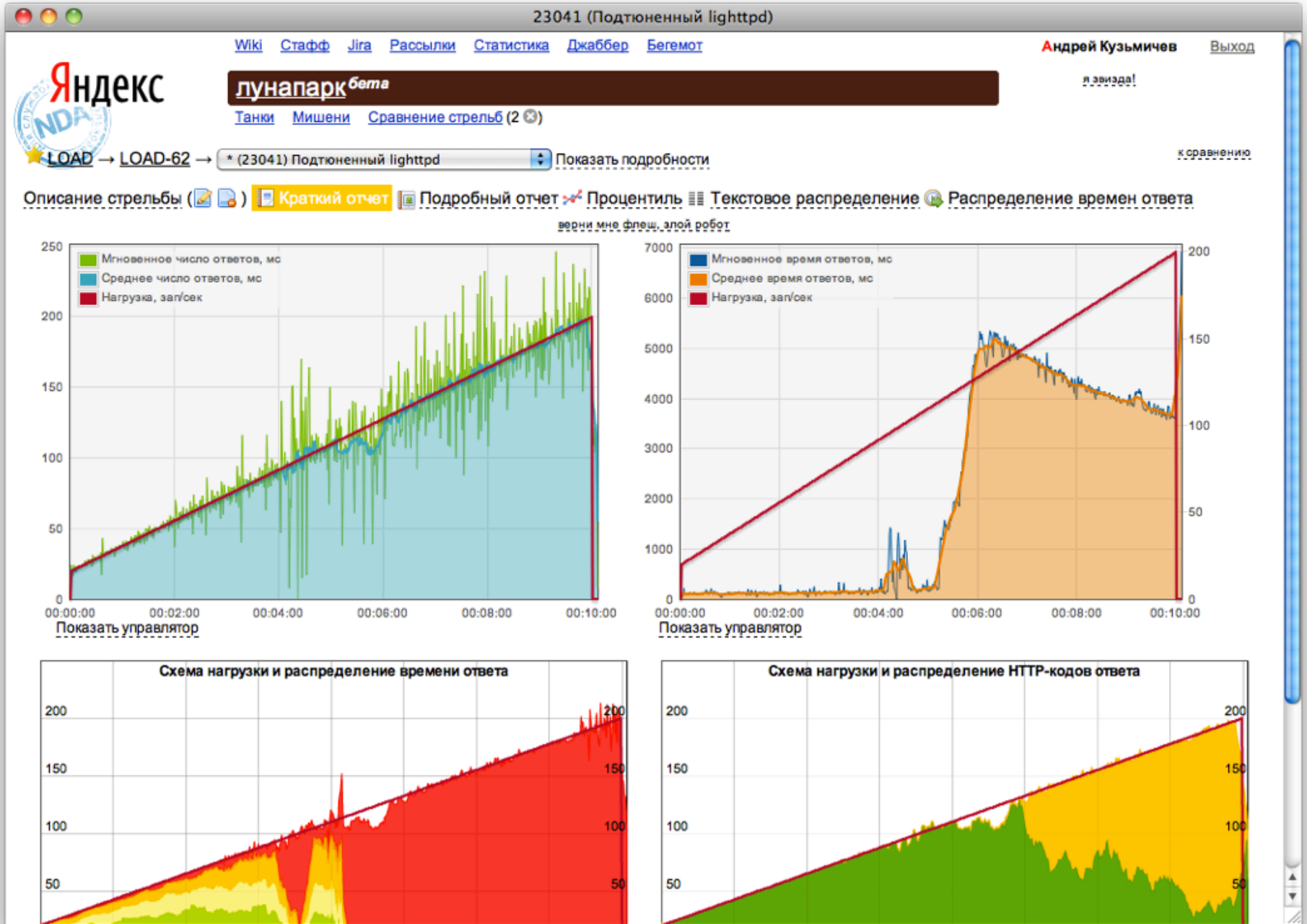
Радость!

Я

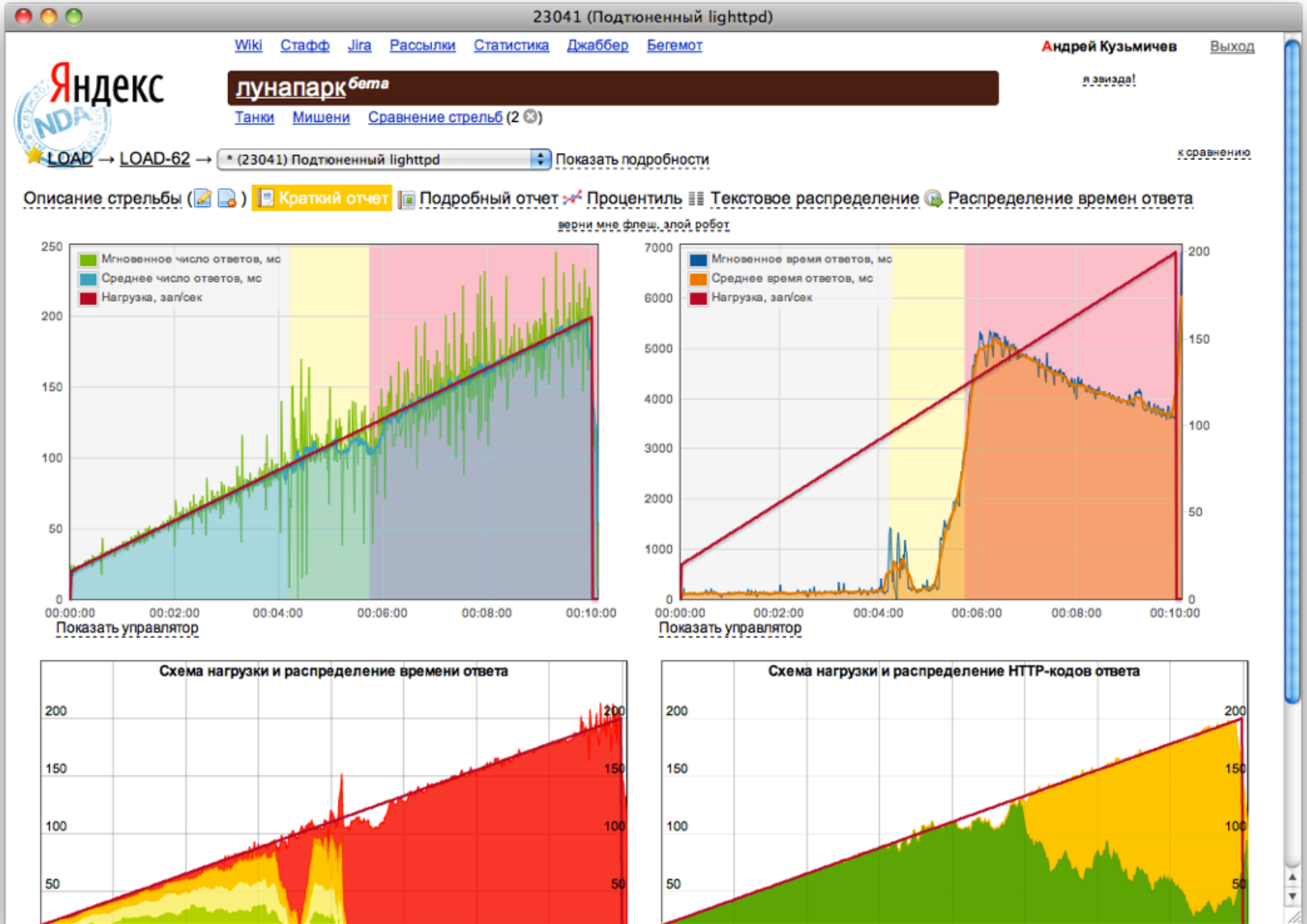
4. Рассмотрим повседневную задачу
5. Проведем аналогии
6. Общий подход к построению хорошего мониторинга
7. Примеры

Лунапарк

Автоматическое выявление разладок



Автоматическое выявление разладок



Автоматическое выявление разладок

При анализе используется время ответа,
HTTP- и сетевые коды ответов

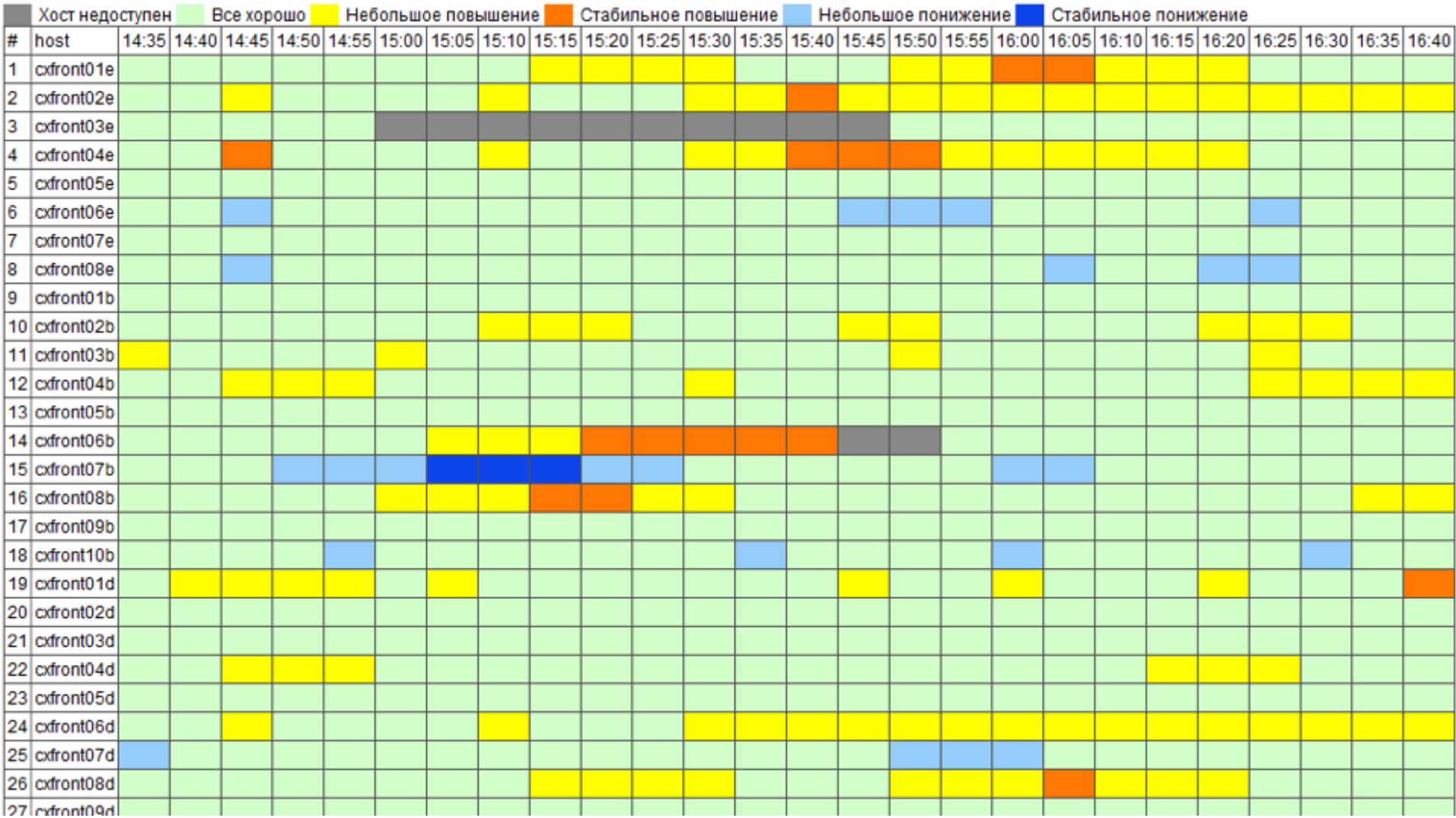
Обучение на 500 размеченных тестах

Точность обнаружения разладки **около 97%**
при вероятности **ложного срабатывания <1%**

Я

Мониторинг продакшн-кластера

Я



#	host	14:35	14:40	14:45	14:50	14:55	15:00	15:05	15:10	15:15	15:20	15:25	15:30	15:35	15:40	15:45	15:50	15:55	16:00	16:05	16:10	16:15	16:20	16:25	16:30	16:35	16:40
1	cxfront01e																										
2	cxfront02e																										
3	cxfront03e																										
4	cxfront04e																										
5	cxfront05e																										
6	cxfront06e																										
7	cxfront07e																										
8	cxfront08e																										
9	cxfront01b																										
10	cxfront02b																										
11	cxfront03b																										
12	cxfront04b																										
13	cxfront05b																										
14	cxfront06b																										
15	cxfront07b																										
16	cxfront08b																										
17	cxfront09b																										
18	cxfront10b																										
19	cxfront01d																										
20	cxfront02d																										
21	cxfront03d																										
22	cxfront04d																										
23	cxfront05d																										
24	cxfront06d																										
25	cxfront07d																										
26	cxfront08d																										
27	cxfront09d																										

Я

Атаки на систему авторизации

Не только “да/нет”...

...но и масштаб проблемы

5
4
3
2
1
0
10.21 06:42
13:42
20:42
10.22 03:42
10:42
17:42
10.23 00:42
07:42
14:42
21:42
10.24 04:42
11:42
10.24 18:42

Я

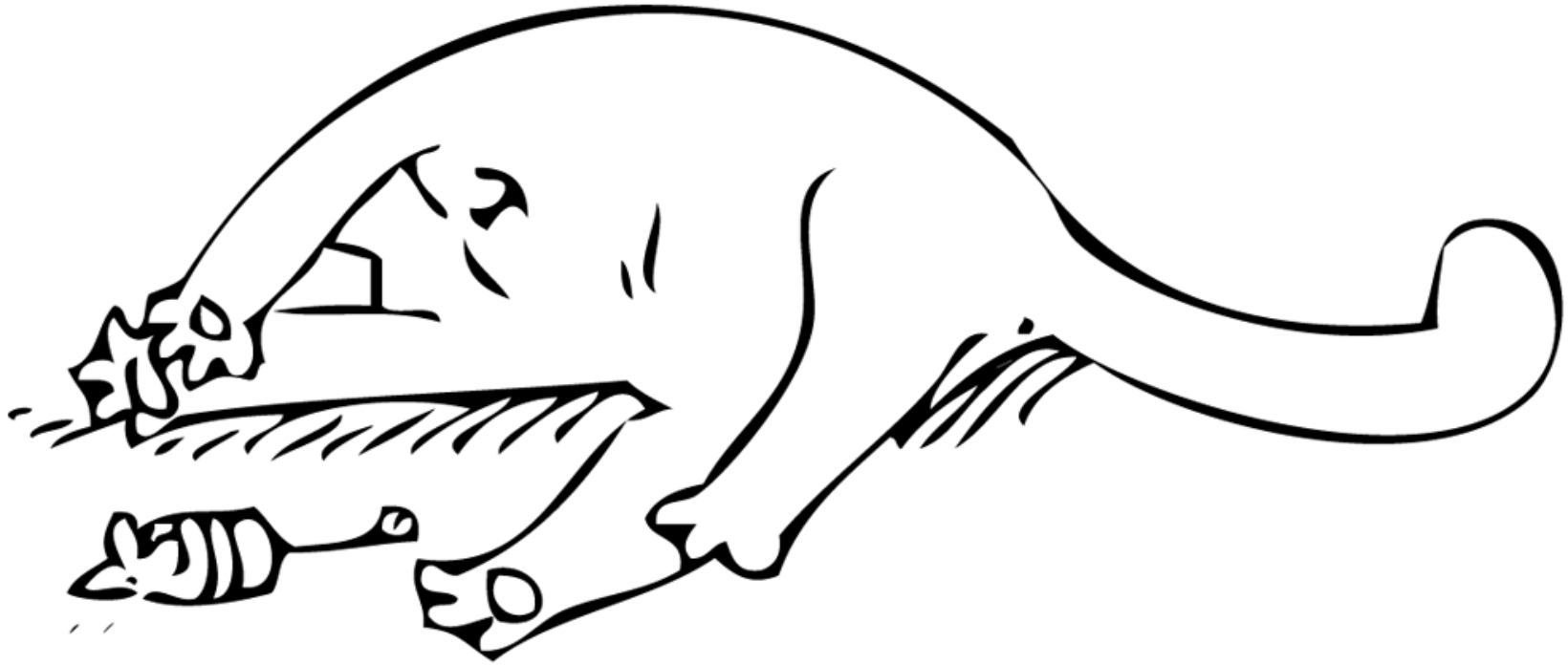
Умный мониторинг

— Математически доказанная эффективность;

— Масштабируемость;

— Гибкость настройки.

Вопросы?



Я

Алиса Смирнова,
Дима Никоненко,
Женя Бурнаев
Группа нагрузочного тестирования

119021, Россия, Москва,
ул. Льва Толстого, д. 16

+7 (495) 739-00-00
+7 (495) 739-70-70 — факс

zero@yandex-team.ru

nikonenko@yandex-team.ru

Процедура скорейшего обнаружения разладки

- Пусть $(X_t)_{t\geq 0}$ наблюдаемый в режиме реального времени пуассоновский поток, у которого в неизвестный момент времени θ интенсивность меняется со значения λ_0 на значение $\lambda_1 \neq \lambda_0$ (λ_0 и λ_1 считаются известными)
- Задаем значение параметра $T > 0$ - среднее время до ложной тревоги
- Определяем значение порога $A = A(T)$
- Подсчитываем значения процесса $\psi_t = \psi_t(X_s, 0 \leq s \leq t)$ по формуле

$$\psi_t = \int_0^t \left(\frac{\lambda_1}{\lambda_0}\right)^{X_t - X_s} e^{-(\lambda_1 - \lambda_0)\cdot(t-s)} ds$$

- Объявляем тревогу (появление разладки) в момент, когда в первый раз будет выполнено неравенство $\psi_t \geq A$