Безопасность и надежность программного обеспечения в техногенном мире

Владимир Обризан
Директор Design and Test Lab
Директор Первого института надежного программного обеспечения

28.08.2017 — Cybersecurity Meetup #1, Харьков

Биография

2005 — инженер-аналитик компьютерных систем, ХНУРЭ

2005 — основал Design and Test Lab

2005-2008 — аспирантура ХНУРЭ

2005-2016 — преподаватель ХНУРЭ

2011 и по сей день — директор Design and Test Lab

2017 — защитил диссертацию к. т. н., ХНУРЭ

2017 — основал Первый институт надежного программного обеспечения

9/9

0800 Arctan started { 1.2700 9.037 847 025
1000 " stopped - arctan ✓ 9.037 846 995 correct
13"sec (032) MP - MC ~~1.9826447000~~ ~~2.13047641S (-3)~~ 4.6159250S9(-2)
(033) PRO 2 2.13047641S
correct 2.13067641S

Relays 6-2 in 033 failed special speed test
in relay " 10.00 test.
Relays changed

Relay 2145
Relay 3370

1100 Started Cosine Tape (Sine check)
1525 Started Mult + Adder Test.

1545  Relay #70 Panel F
(moth) in relay.

First actual case of bug being found.

~~1715~~ 1630 Arctangent started.
1700 closed down.

ЄДБО, 2017

Онлайн-система приема заявлений абитуриентов (Украина).

В результате сбоя утрачено 40,000 заявлений абитуриентов.

«Заявлений о поступлении не видно, но это не значит, что их нет в базе. Они просто не высвечиваются. Абитуриенты получат на свою электронную почту или в электронные кабинеты в ЕГЭБО сообщения о том, что надо подать заявление еще раз»

NASDAQ, 2012

Facebook IPO: продано акций на 18 млрд долларов.

В результате программного сбоя в течение нескольких часов трейдеры не могли узнать состояние заявок: прошли или отменены.

Программисты «исправили» ошибку. После обновления ПО 30,000 заявок все еще находились в «подвешенном» состоянии в течение двух часов.

Позже NASDAQ выплатила 72 млн долларов трейдерам в виде штрафов.

Аэропорт Хитроу, 2008

Стоимость постройки Терминала №5 — 8,5 млрд долларов.

180 айти-компаний поставили 163 системы.

9000 устройств, 2100 ПК.

Из-за ошибки в работе айти-системы были отменены 300 авиарейсов на протяжении 5 дней.

Айти-система управления багажом ошибочно сообщила грузчикам, что рейсы уже улетели. Тем самым багаж не был погружен в самолеты и был возвращен обратно в терминал. В результате пассажиры улетели без багажа, а сам терминал был переполнен неотправленным багажом.

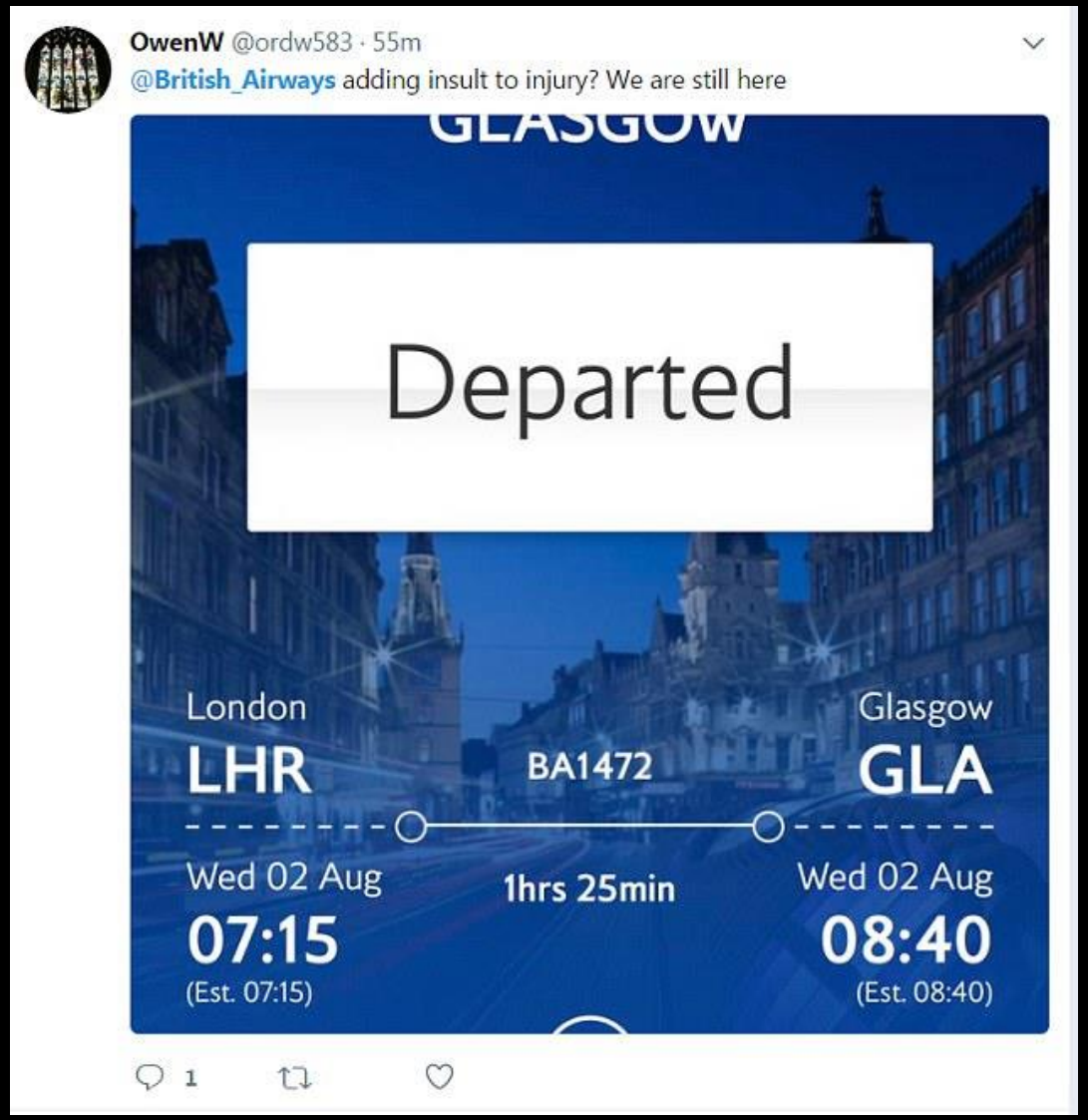
Один из грузчиков: «В течение последних нескольких недель проводились тесты ленты, и мы знали о существующих проблемах».

Британские авиалинии, 2017

Семь технических сбоев за 2017 год.

Жалобы:

- Отмена авиарейсов
- Невозможность распечатать посадочный талон
- 1,5-часовая очередь на сдачу багажа
- Сбои в работе мобильного приложения



Тойота, 2010

Отказ тормозной системы в Приусе из-за ошибки в программном обеспечении.

102 жалобы водителей.

2 ДТП, 2 пострадавших.

Ошибка исправлена установкой обновления ПО.

Тойота, 2015

Тойота отозвала 625,000 Приусов.

Причина: «Ошибка в программном обеспечении могла привести к отказу гибридной системы во время движения».

428 жалобы водителей.

Тесла, 2016

Водитель погиб в ДТП в то время, когда автомобиль был в режиме автопилота.

Причина: «Автопилот не заметил трактор».

Stuxnet, 2010

Stuxnet — компьютерный вирус (червь).

Цель атаки — иранская ядерная программа.

Действие — перехватывает команды управляющей программы, поступающие на промышленное оборудование (центрифуги), модифицирует команды таким образом, что центрифуги выходят из строя.

Эффект, по разным сообщениям:

- производственные мощности упали на 30%
- количество центрифуг сократилось с 4700 до 3900
- 1000 центрифуг уничтожены

Что, если программисты станут врачами?

— Доктор! У меня нога болит!

— Странно, а у меня такая же нога и не болит.

Therac-25, 1985

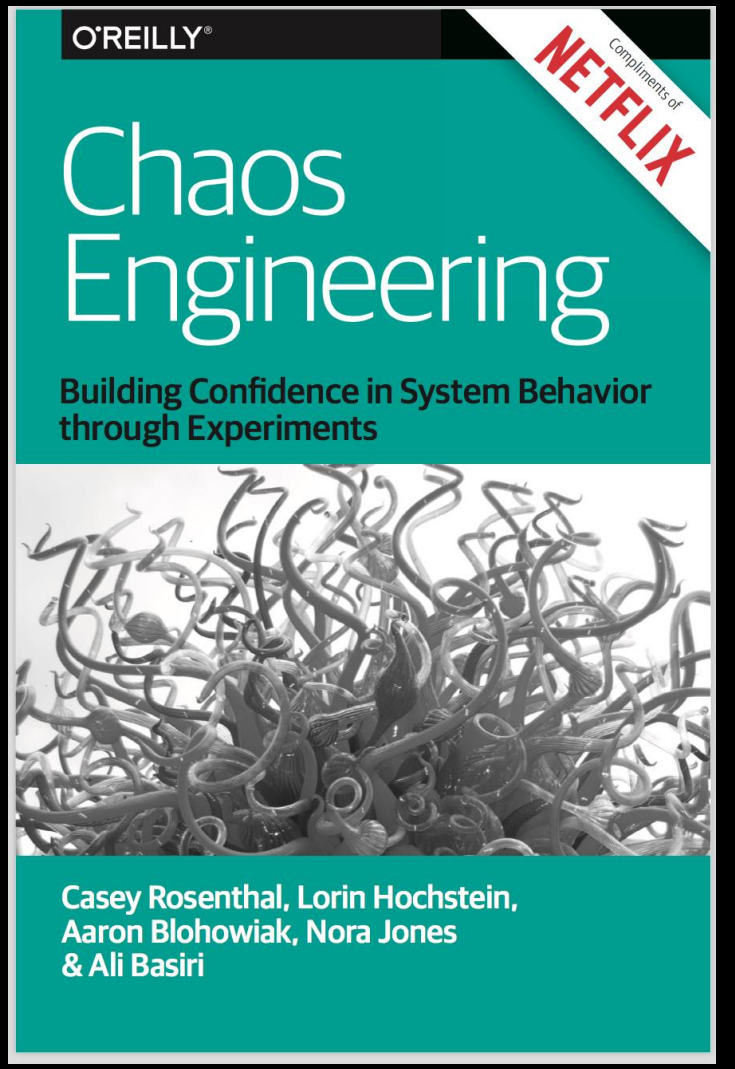
В период с 1985 по 1987 — шесть случаев передозировки излучением.

Минимум две смерти от лучевой болезни.

Причина — ошибка в управляющей программе.

Разработчик аппарата неоднократно заявлял, что передозировка невозможна.


JULY/AUGUST 2017
VOL. 34, NO. 4
IEEE
Software
200th ISSUE
RELIABILITY ENGINEERING
WHAT TYPE OF PEOPLE ARE SOFTWARE ARCHITECTS? // 20
DEAD PROGRAMS // 80
IEEE
IEEE computer society
WWW.COMPUTER.ORG/SOFTWARE


O'REILLY®
Compliments of
NETFLIX
Chaos Engineering
Building Confidence in System Behavior through Experiments
Casey Rosenthal, Lorin Hochstein, Aaron Blohowiak, Nora Jones & Ali Basiri

Плохой пример отношения

[redacted] 18:55

Здравствуйте Владимир,меня зовут [redacted] я веб-программист.
Посмотреть выполненные мною работы,почитать обо мне отзывы вы можете в моем профиле на фрилансе
http://freelance.ru/[redacted]

Владимир 19:35

Добрый день, [redacted]! Спасибо за сообщение! Мы сейчас ищем PHP-программиста, frontend-программиста в офис в Харькове. Вам это интересно?

[redacted] 19:40

я backend разработчик

Владимир 19:41

На каких технологиях?

[redacted] 19:41

Зависит от бюджета

вам нужен стандартный проект на php7,yii2,mysql?
Или вам требуется проект под высокую нагрузку с помощью php7,yii2,mongodb ?
Разница в том что когда в стандартном проекте в таблице которая связана с другими будет более 100 тысяч записей имеется вероятность что запросы будут выполняться намного медленее.
И для лечения подобной проблемы вам необходимо будет подключать кэширование запросов.
А при разработке сразу под высокую нагрузку архитектура будет разработана таким образом чтобы она могла легко выдержать любую нагрузку без необходимости "доработки проекта"
И соответственно цена этих двух подходов разная.
Разработка под высокую нагрузку значительно дороже стандартного проекта

Владимир 19:42

Согласен.

У вас есть опыт с высокой нагрузкой?

[redacted] 19:42

Да

об этом написано

в моем профиле на фрилансе

Изначально я разрабатывал всегда под высокую нагрузку на yii2,mongodb

Сейчас я изменил полностью политику и разрабатываю как стандартные проекты так и под высокую нагрузку

Все зависит от бюджета

Потому что человеку очень сложно обьяснить почему mongodb это хорошо

а mysql плохо

лучше всего за это говорят деньги)

Владимир 19:44

Я вижу описание проекта с 10 000 товарами. А сколько визитов этот сервис выдерживает?

[redacted] 19:45

статистику посещений я у клиента не брал

исход был в том что за все время он не написал о каких либо проблемах

соответственно все хорошо

Владимир 19:45

Высокая нагрузка — это ж не сколько товаров в базе лежит (10 000 это смешно кстати), а сколько пользователей с этими данными работают.

"соответственно все хорошо"
Это заблуждение.

[redacted] 19:46

Заблуждаетесь вы

речь идет о архитектуре

а о том как идет поддержка

это две разные вещи

и зависят напрямую от подходов к архитектуре

Владимир 19:46

Если вы не делали нагрузочных тестов, и не имеете статистики по производительности, то обсуждать архитектуру нет смысла.

[redacted] 19:47

Все сугубо индивидуально и зависит от бюджета и сроков

Поэтому выводов на основе умных слов делать не нужно.

и про нагрузочные тесты и про все остальное я прекрасно знаю

Владимир 19:50

Еще раз вопрос: можете ли вы показать проект с высокой нагрузкой, с измеренными параметрами? Кол-во визитов, время ответов от сервера?

[redacted] 19:50

Для вас нет

вы внимательно прочитайте про что идет речь

и не подменяйте понятия

Владимир 19:51

Вот смотрите требования, которые мы выставил мой клиент:

[redacted] 19:51

скидывайте требования

Скорость ответа сервера измеряется не только кодом написаным,но и полностью настройкой сервера

Владимир 19:52

It currently handles per year:

- 1.2 million unique visitors
- 2.7 million visits
- 3.8 million pages viewed
- 1.8 million videos viewed
- 37.5 million minutes viewed

[redacted] 19:52
и соответственно чтобы говорить об этом,мне еще нужно подключать системного администратора

Владимир 19:52
Еще требование, что специалист должен пройти собеседование с техническим диреткором, который уже это разработал.

[redacted] 19:52
В стандартных же случаях,в рамках этого системного администратора выступает хостер

У вас очень крупный проект насколько я понимаю.

Владимир 19:53
Да.

Владимир 19:54

У вас есть опыт системного администрирования высоконагруженных проектов?

[redacted] 19:54

нет

[redacted] 19:54

У меня есть опыт построения архитектуры

а поддержкой всегда занимались хостеры

В рамках этого,соответственно я снижаю риски высокой нагрузки

но расширением вертикальным или горизонтальным

это сугубо задача системного администратора.

Так как например делая на mysql для вертикального масштабирования проекту нужно дополнительно подключать кэширование

а в случае с mongodb делать это не нужно,так как это продумано сразу в рамках архитектуры приложения

в этом и есть разница

что в случае с mysql вам нужен полюбому прогер и системный администратор

а для монго достаточно просто системного администратора

про mysql возможно я описал очень поверхностно

так как там есть еще инструменты в виде индексации и т.д

но главную суть я думаю вы поняли,про что я имею ввиду.

Еще один пример

Marco Rodzynek
CEO at NOAH, Conference Organizer, M&A Advisor, Angel Investor, Entrepreneur
5d

Do not work with the IT outsourcer Ciklum. We lost a little fortune with them and did not get any product even after doubling the project time. Maybe it works for others, but it certainly did not work for us. Contracts won't help you here.
Take care Marco

260 Likes • 81 Comments

Like Comment Share

Konstantin Chernov Looks like a bunch of guys (allegedly from the mentioned Ciklum) are making same argument like 'Ciklum is not an outsourcing, its out-staffing company, so it has zero responsibility'. Very suspicious.

Like Reply

Institute of
Reliable
Software

Первый институт надежного программного обеспечения

формирует новую культуру IT-проектирования

Меморандум целей

Institute of Reliable Software

1. Формирование и пропаганда новой культуры IT-проектирования:
надежно; wow-код; personally signed quality.

2. Внедрение нового института стандартов разработки и надежного программирования.

3. Популяризация знаний в области надежного IT-проектирования, обеспечивая свободный доступ к ним.

4. Формирование профессионального сообщества IT-специалистов объединенных высокими профессиональными, моральными и этическими принципами организации проведения работ в области создания надежных IT-продуктов.

5. Введение нового стандарта оценки профессионализма программистов.

6. Пропаганда этики профессиональной гордости и ответственности за созданный проект.

7. Разработка и распространение стандарта IRS-2020 — нового стандарта надежного IT-проектирования.

Контакты

Владимир Обризан

Первый институт надежного программного обеспечения

facebook.com/1stIRS