ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛАЭКОНОМИКИ»

*Высшая школа бизнеса*

Волков Андрей Андреевич

**РАЗРАБОТКА СИСТЕМЫ ДЛЯ ПОСТРОЕНИЯ МОНИТОРИНГА,**

**АНАЛИЗА АНОМАЛИЙ И СВОЕВРЕМЕННОГО ПРЕДУПРЕЖДЕНИЯ**

**ДЛЯ СОВРЕМЕННЫХ IT КОМПАНИЙ**

Выпускная квалификационная работа

по направлению подготовки 38.03.05 Бизнес-информатика

образовательная программа «Бизнес-информатика»

|  |  |
| --- | --- |
|  | Научный руководитель |
|  | к.т.н, доцент |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | С. Г. Ефремов |

Москва 2021

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc39691355)

[ВВЕДЕНИЕ. 4](#_Toc39691356)

[Актуальность. 4](#_Toc39691357)

[Цель исследования. 5](#_Toc39691358)

[Задачи исследования. 5](#_Toc39691359)

[Методы. 6](#_Toc39691360)

[ГЛАВА I. Предметная область мониторинга бизнес-приложений. 7](#_Toc39691361)

[1 Мониторинг бизнес-приложений. 16](#_Toc39691370)

[1.1 Используемая терминология. 16](#_Toc39691371)

[1.2 Задачи систем монитоирнга. 18](#_Toc39691372)

[1.3 Проблематика предметной области. 19](#_Toc39691373)

[2 Работа с метриками. 16](#_Toc39691370)

[2.1 Симптомы и причины. 16](#_Toc39691371)

[2.2 Методы черного и белого ящика. 18](#_Toc39691372)

[2.3 4 золотых сигнала. 18](#_Toc39691372)

[2.4 Перцентили и работа с выбросами в метриках. 19](#_Toc39691373)

[2.5 Уровень детализации измерений. 19](#_Toc39691373)

[2.6 Долгосрочное наблюдение. 19](#_Toc39691373)

[2.7 Раскрытие понятия SRE и соглашения: SLA / SLO / SLI. 19](#_Toc39691373)

[2.8 Инфраструктура как код (Infrastructure as a code). 19](#_Toc39691373)

[3 Архитектура мониторинговых систем. 16](#_Toc39691370)

[3.1 Инструменты для экспорта и сбора метрик приложения 16](#_Toc39691371)

[3.2 Метки в метриках 18](#_Toc39691372)

[3.3 Хранение метрик временных рядов 19](#_Toc39691373)

[3.4 Существующие системы мониторинга бизнес-приложений 19](#_Toc39691373)

[ГЛАВА 2. Архитектура сервиса 16](#_Toc39691369)

[ЗАКЛЮЧЕНИЕ 46](#_Toc39691395)

[СПИСОК ЛИТЕРАТУРЫ 47](#_Toc39691396)

# ВВЕДЕНИЕ

***Актуальность***

В современном мире все больше компаний переходят на онлайн модель ведения бизнеса, сегодня бизнес в любой сфере – начиная с новостей, кино, обучения и заканчивая банками, фондовыми биржами – более удобен для клиентов в онлайн, чем в оффлайн формате. За каждым таким IT бизнесом стоит отдельная группа приложений, которые, общаясь между собой и сторонними системами, обеспечивают работу современных IT компаний.

Однако далеко не всегда такую работу можно назвать надежной, в современном мире большое количество проблем, связанных с доступностью приложений и с корректностью выполнения их бизнес-логики.

Проблемы с доступностью могут возникать по целому ряду причин. Например, возникли проблемы с сетью, сервис под нагрузкой стал медленнее отвечать, приложение начало требовать больше ресурсов, произошел сбой в инфраструктуре. Во всех этих случаях бизнес получает один и тот же результат – сервис недоступен.

Проблемы с корректностью выполнения бизнес-логики приложения тоже могут возникать по множеству разных причин, в зависимости от конкретного бизнеса причины будут специфические. Для примера возьмем онлайн банк, который открывает новые дебетовые счета и выдает кредиты. В такой банковской IT системе мы можем перестать отправлять уведомления об открытии нового счета, начать выдавать кредиты на большие суммы людям с низким уровнем кредитоспособности, одобрять кредиты на небольшие суммы людям с высоким уровнем кредитоспособности и так далее. Во всех этих случаях бизнес получает один и тот же результат – аномальное поведение со стороны бизнес-логики.

Интересно то, что такие проблемы, если они не массовые, бывает очень сложно обнаружить. Например, в случае отказа одного стороннего сервиса, наше приложение стало обрабатывать запросы в два раза дольше, а мы этого можем даже не узнать. В случае с банком 0.5% клиентам может не приходить уведомление об открытии счета при специфических входных параметрах, то есть в целом система работает – видно, что счета открываются и часть клиентов ими пользуются, при этом бизнес может даже не подозревать о том, что на самом деле каждый день теряем весомый процент потенциальной прибыли.

Решением подобного рода проблем является мониторинг приложений. Мониторинг – сбор, обработка, агрегирование и отображение в реальном времени количественных показателей системы, например общее число и тип запросов, количество ошибок и их типы, время обработки запросов и время функционирования серверов (SRE book).

Мониторинг позволяет профилировать приложение на каждом из этапов его работы, экспортировать и собирать технические и бизнес метрики приложения. Благодаря мониторингу, обнаружению аномалий и своевременному оповещению, можно добиться прозрачного представления о работе приложения и вовремя реагировать на появление проблем с его работой.

***Цель работы***

Целью данной работы является разработка системы для построения мониторинга, анализа аномалий и своевременного предупреждения со следующими свойствами:

1. Программный API для создания и экспорта метрик
2. Развертывание облачной инфраструктуры для сбора и построения графиков с метриками
3. Реализация алгоритмов для анализа аномалий во временных рядах и экспорт метрик с аномалиями
4. Построение графиков в пользовательском интерфейсе посредством программного API
5. Пользовательский интерфейс для отображения графиков с метриками приложения
6. Система предупреждения, отправляющая уведомления о сбоях в популярные мессенджеры

***Объект и предмет исследования***

Объект исследования: экосистема мониторинга приложения.

Предмет исследования: API для построения метрик, алгоритмы для анализа аномалий, система оповещения о сбоях.

***Задачи*:**

* Изучить существующие подходы к реализации мониторинга в приложениях и существующие инфраструктурные решения;
* Определить требования к системе для построения мониторинга со стороны конфигурации метрик, анализа аномалий, пользовательского интерфейса, инфраструктуры;
* Изучить алгоритмы для анализа аномалий во временных рядах;
* Разработать API для написания и конфигурации метрик;
* Развернуть инфраструктуру для экспорта, сбора и отображения метрик в режиме реального времени;

***Методы***

В рамках работы будут проанализированы работы на тему мониторинга и анализа аномалий, а также использован опыт крупных компаний из различных IT сфер. На основе этих знаний будут составлены требования к системе и определены ограничения к ее функционалу. Описанная система будет разработана и задокументирована.

# Глава 1. Предметная область мониторинга бизнес-приложений

**1.1. Мониторинг бизнес-приложений**

* + 1. Используемая терминология

Мониторинг – сбор, обработка, агрегирование и отображение в реальном времени количественных показателей системы, например общее число и тип запросов, количество ошибок и их типы, время обработки запросов и время функционирования серверов.

Оповещение – сообщения, на которые должен обратить внимание человек и которые направляются в конкретную систему, например в очередь запросов («тикетов»), в электронную почту или на специальное устройство — пейджер.

SRE (Site reliability engineering) - это дисциплина, которая включает аспекты разработки программного обеспечения и применяет их к инфраструктуре и операционным проблемам.

Приложение (сервис) – компьютерная программа, написанная программистом, которая подчиняется, заложенной в нее бизнес-логике и удовлетворяет потребности клиентов.

* + 1. Задачи системы мониторинга

С помощью системы мониторинга решается множество различных задач, особенно выделить можно следующие:

* *Анализ долгосрочных тенденций.* Мониторинг позволяет оценивать тренды в долгосрочной перспективе, например, сравнение размера базы данных сегодня и полгода назад даст представление о скорости ее заполняемости, а сравнение кол-ва обработанных запросах может сказать росте или снижении популярности приложения.
* *Сравнение с предыдущими версиями или экспериментальными группами.* Сравнение производительности разных версий приложения позволит сопоставить значения ключевых метрик приложения и отдать предпочтение той или оной технологии / методу. Например, новая версия веб-фреймворка может работать медленнее предыдущей версии, что повлияет на решение «откатиться» на предыдущую версию, пока не будет исправлена новая.
* *Оповещение.* Наблюдение за ключевыми метриками доступности приложения может сообщить о сбое или о его предпосылках, что позволит вовремя оповестить инженеров о неисправности и спровоцировать реакцию на инцидент. Например, сервис начали больше использовать, и он стал потреблять близкое к пороговому значению кол-во ресурсов, в таком случае инженеры должны вмешаться в ситуацию и либо снизить нагрузку на сервис, либо увеличить кол-во доступных ресурсов для приложения.
* *Создание информационных панелей.* Любую метрику – будь то техническая метрика или бизнес-метрика – можно интегрировать в информационную панель. Данная панель должна содержать ответы на главные вопросы о работе сервиса. Например, на панели могут быть изображены графики скорости обработки запросов или их классификация по бизнес-признакам.
* *Ретроспективный анализ различного назначения.* Ретроспективный анализ позволяет выявлять причинно-следственные связи между различного рода событиями. Например, время ответа сервиса резко возросло вдвое, в то же время резко возросла скорость выполнения запросов в базу данных, в то же время увеличилось кол-во ошибок при попытке установить соединения с базой данных, что свидетельствует о проблемах на сети. Значит, если устранить первоначальную проблему, то можно решить ее следствие.
  + 1. Проблематика предметной области

Основная проблема, которую решает мониторинг – возможность технического и бизнес профайлинга приложений. Мониторинг делает процессы прозрачными, доступными для анализа. Вместе с системой оповещения мониторинг позволяет вовремя сообщать о возникшей или ожидающейся неисправности.

* 1. **Работа с метриками**
     1. Симптомы и причины

При анализе метрик любая система мониторинга отвечает на два вопроса: что сломалось и почему это сломалось. Ответ на вопрос «Что сломалось?» подразумевает под собой определение симптома проблема, а ответ на вопрос «Почему это сломалось?» определяет причину этой проблемы. В таблице приведены примеры симптомов и соответствующих им причин.

|  |  |
| --- | --- |
| **Симптом** | **Причина** |
| Сервис возвращает ответы HTTP 408 | Сторонний сервис начал долго обрабатывать запросы |
| Сервис возвращает ответы HTTP 401 | Сервис авторизации изменил алгоритм шифрования токенов |
| Время ответа сервиса увеличилось вдвое | База данных начала испытывать аномальное кол-во запросов от других сервисов |
| Сервис использует в 1.5 раза больше ресурсов по памяти | Выросло кол-во одновременно обрабатываемых запросов |

Хорошо сделанная система мониторинга должна выявлять причинно-следственные связи «что» и «почему» и демонстрировать их инженерам.

* + 1. Методы черного и белого ящика

В любой системе мониторинга широко используются методы черного и белого ящика. Метод черного ящика заключается в наблюдении за симптомами, которые выявляют реально возникшие проблемы. Метод белого ящика – это возможности наблюдать за внутренним устройством системы. Метод белого ящика позволяет обнаруживать потенциальные проблемы, а метод черного ящика работает с существующими проблемами.

Обратим внимание, что в многоуровневой системе то, что можно классифицировать как симптом для одной системы, для другой системы может являться причиной. Например, если у сервиса «a» вдвое выросло время ответа и этот факты является симптомом для сервиса «a», то для сервиса «b», который вызывает сервис «a» данный факт будет причиной. Поэтому очень важно проводить причинно-следственные связи, чтобы искать проблему не в соединении между двумя сервисами, а сразу исследовать симптом сервиса «a».

Метод черного ящика хорошо применять для экстренных оповещений, поскольку такое оповещение произойдет только в том случае, если проблема уже точно существует и дает реальные симптомы. Однако для потенциальных проблем более уместен метод белого ящика с правильно подобранными пороговыми значениями для реагирования.

* + 1. 4 золотых показателя

«Четыре золотых показателя» для системы мониторинга являются: время ответа, величина трафика, уровень ошибок и степень загруженности. Это основные метрики для минимальной диагностики работы любого сервиса. Рассмотрим каждый из них подробнее.

* *Время ответа.* Время, которое необходимо для выполнения запроса. В данной метрике очень важно разделять время ответа для успешных и неуспешных запросов. Например, код ошибки 401 Unauthorized возвращается очень быстро, однако, поскольку данный код ответа указывает на то, что запрос не был выполнен, то учитывать данный запрос при подсчете общей статистике некорректно.
* *Величина трафика.* Величина нагрузки, которую обрабатывает сервис. Для разных сервисов единицы измерения нагрузки будут разными, например, для веб-сервиса трафик измеряется в количестве HTTP запросов в секунду, для сервиса, который читает очередь брокера сообщений – количество прочитанных сообщений, для системы потокового аудио сигнала это скорость передачи данных по сети или количество параллельных соединений.
* *Уровень ошибок.* Количество неуспешно выполненных запросов: явно (возвращаемый код не относится к категории успешных – не 2\*\*), неявно (если код ответа является успешным, но полученные данные являются неправильными) или не соответствующих требованиям (например, если ответ должен приходить в пределах 2-ух секунд, то любой запрос, выполнившийся за большее время считается неуспешным)
* *Степень загруженности.* Показатель того, насколько сильно загружен сервис. В каждом сервисе это сразу набор метрик, которые показывают ограничения в работе сервиса, например, в приложении, ограниченных по ресурсам – это ресурсы, в приложениях имеющих ограничения на количество одновременно выполняемых запросов – это количество потоков в очереди пула потоков. Отметим, что многие сервисы начинают работать медленнее еще до того, как перейдут пороговое значение по своей степени загруженности, поэтому очень важно следить за данными метриками как за целевым показателем.

Если удается измерить все четыре сигнала и сообщить клиентам о том, что один из них находится вне своей нормы, то качество мониторинга для сервиса можно определить как минимум удовлетворительным.

* + 1. Перцентили и работа с выбросами в метриках

При разработке системы мониторинга есть большой соблазн использовать для метрик средние значения: среднее время обработки запроса, средний процент загрузки сервиса, среднюю заполненность базы данных и т. д. Риски, связанные с такой оценкой заключаются в том, что средние значения могут скрывать проблемные места в работе сервиса. Например, среднее время обработки запроса может быть в пределах нормы – 300 миллисекунд, однако из 1000 запросов 5% отвечают за 3 секунды, а 10% за 1 секунду.

Самый простой способ различать медленное среднее время обработки и крайне медленные «хвосты» - вместо значений задержки использовать кол-во запросов, величина задержки которых попадает в заданные интервалы (бакеты), удобные для построения гистограммы: какое количество запросов потребовало для обработки от 0 до 100 миллисекунд, от 100 до 300, от 300 до 700 и т. д. Построение гистограмм с логарифмически расставленными границами интервалов (с основанием, приблизительно равным 3) – один из самых простых и эффективных способов наглядно продемонстрировать распределение характеристик запросов к сервису.

* + 1. Уровень детализации измерений

Для разных компонентов системы измерения должны проводиться с разным уровнем детализации. Например, контроль загрузки центрального процессора с периодичностью в минуту будет нерепрезентативной метрикой, а, например, проверка доступности сервиса с той же периодичностью будет качественной метрикой, поскольку результат наблюдения меняется не так часто.

Важно подходить к детализации каждой метрики отдельно и экспериментировать с настройками скрейпинга (англ. scrape – царапать).

* + 1. Долгосрочное наблюдение

Мониторинг обеспечивает слежение за постоянно меняющимися системами, у которых меняется степень нагрузки и целевой уровень производительности. Важно, чтобы при построении мониторинга для приложений инженеры руководствовались долгосрочными перспективами. При определении целевых показателей часто придется прибегать к компромиссным решениям, отказываться от высоких показателей доступности, чтобы иметь возможность и время улучшить данные показатели в будущем.

* + 1. Раскрытие понятия SRE и соглашения: SLA / SLO / SLI
    2. Инфраструктура как код (Infrastructure as a code)
  1. Архитектура мониторинговых систем
     1. Инструменты для экспорта и сбора метрик приложения
     2. Метки в метриках
     3. Хранение метрик временных рядов
     4. Существующие системы мониторинга бизнес-приложений
  2. Аномалии во временных рядах
     1. Раскрытие понятия, примеры аномалий во временных рядах
     2. Методы анализа аномалий
     3. Системы предупреждения и процесс реагирования на аномалии
     4. Существующие системы анализа аномалий

# Глава 2. Архитектура сервиса

1. Требования к системе мониторинга
   1. Требования к инфраструктуре для развертывания, приложения на языке Java
   2. Ограничения системы