DataScience трансформация: системы мониторинга как аналитический инструмент для ИТ. Применение в промышленности

И.В. Шутов (Компания Техносерв)

Проанализирована ситуация в области решения задач управления вычислительными мощностями на промышленных предприятиях. Отмечается, что происходит смещение акцентов с задачи сбора данных и аварий в сторону обработки информации. Показано, как все современные тенденции отражаются в системах мониторинга ИТ-инфраструктуры нового поколения, в том числе в системе t.Mon.

Ключевые слова: информационные технологии, вычислительные ресурсы, сбор данных, обработка информации, мониторинг ИТ-инфраструктуры.

Мы живем в достаточно интересное время с точки зрения событийной насыщенности, смены парадигм и разрушения старых моделей, казавшихся незыблемыми. Это касается как глобальной плоскости, включающей политическую перестройку мира, смену экономических моделей, так локальных плоскостей в различных областях человеческой деятельности.

Большинство происходящих изменений хорошо укладываются в концепцию развития ноосферы, предложенной В. И. Вернадским еще в начале XX века. Отдельный класс изменений касается информационной сферы: получения данных и их обработки, информационного обмена, хранения, использования в рамках других процессов.

В промышленности также происходят значительные сдвиги, но преобразование материальных объектов происходит гораздо медленнее, нежели преобразование нематериальных (информации). Тем не менее, несмотря на исполнение ИТ роли второго плана в промышленности, значимость происходящих изменений никак нельзя не замечать.

В российском промышленном сегменте можно выделить несколько ключевых трендов, связанных с использованием ИТ и вполне коррелирующих (с определенной временной задержкой) с прогнозами ведущих аналитических агентств:

- нивелирование роли ИТ до уровня обслуживающего подразделения;
- активное внедрение виртуализации (компьютеры, системы хранения данных, сети);
- смещение акцентов с контроля над процессами на прогнозирование и превентивное недопущение возможных сбоев;
- формирование единых центров управления с детальным мониторингом как технологических, так и информационных процессов, с автоматизацией принятия решений средствами операционной аналитики на основе статистических показателей и алгоритмов с элементами искусственного интеллекта.

Ситуация в ИТ во многом схожа с появлением квантовой механики в начале XX века, когда во вполне ясной и строгой физической модели мира было несколько «мелких» нерешенных вопросов, в частности, проблема в теории излучения черного тела. И для решения этой «маленькой» проблемы пришлось радикально изменить картину устройства мира.

За последние 1,5...2 года в промышленном секторе наблюдался повышенный интерес к задачам управления вычислительными мощностями [1, 2], а также различным запросам предложения/информации (RFI/RFP)[1]. На первый взгляд, ничего необычного, но если взглянуть более пристально, то этот запрос является одним из рычагов проведения серьезных изменений ИТ уровня автоматизации в промышленности.

Во-первых, повышенный интерес к управлению мощностями показывает заинтересованность бизнеса в оптимизации использования ИТ-ресурсов. Закончилась эпоха экстенсивного развития и неограниченного вкладывания средств в ИТ.

Во-вторых, выход на открытый рынок с подобными запросами явным образом декларирует, что бизнес-пользователи как внутренние заказчики нивелируют роль ИТ-специалистов внутри компании до уровня обслуживающего персонала. Задача управления мощностями, требующая широкого подхода, навыков консультантов и использования математического аппарата, не может быть возложена на внутреннее ИТ-подразделение.

[1] Запрос предложения (*Request for Proposal*, RFP) — документированный запрос организации, заинтересованной в приобретении каких-либо товаров или услуг. Создается заказчиком для потенциальных подрядчиков (поставщиков) в тендерных или аукционных процессах.

Запрос информации (*Request for information*, RFI) - запрос предложения от потенциального продавца или поставщика услуг, чтобы определить, какие продукты и службы потенциально доступны на рынке для удовлетворения потребностей покупателя и узнать возможность продавца с точки зрения предложений и сил продавца.

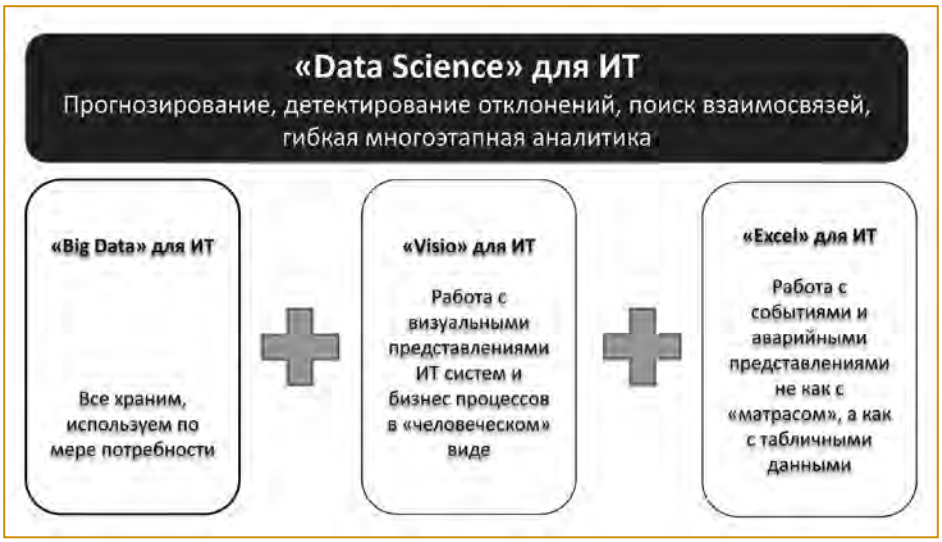

Рис. 1. «Три кита» современной системы мониторинга ИТ

В-третьих, эти запросы формулируются именно в терминах бизнеса. Необходим результат «под ключ» в качестве встроенных блоков в операционные процессы поддержки ИТ в виде выработки рекомендаций (частота может меняться) по внесению изменений в конфигурации, перераспределению ресурсов под изменяющиеся потребности бизнес-заказчиков, модернизацию ПО и «железа». При этом подобный консалтинг не может проводиться методом пристального взгляда или расчетами на салфетках. Необходим прецизионный инструмент в виде систем мониторинга, систем математического моделирования и средств по автоматизации управления конфигурациями ИТ и т. д. Бизнес-заказчиков не интересует абстрактные рассуждения. Важным является только решение конкретной бизнес-задачи.

Таблица. Традиционные подходы к мониторингу не соответствуют современным задачам

Традиционный подход	Современный подход
Сбор аварийных сообщений по факту возникновения проблемных ситуаций	Проактивный мониторинг всех ключевых метрик с требуемой периодичностью опроса (вплоть до секунд)
Жесткая методика сбора данных	Гибкие программно-управляемые подходы к глубине и частоте сбора данных
Основной способ сбора информации – посредством SNMP	Сбор данных с использованием широкого спектра протоколов
Агрегация исторических данных	Хранение исторических данных в исходном виде
Разрозненное информационное поле	Консолидация данных с возможностью аналитической обработки информации от различных источников
Жесткое структурирование зависимостей между элементами и метриками	Использование алгоритмов машинного обучения для выявления скрытых зависимостей между метриками
Отсутствие или слабое функциональное наполнение (следствие малого набора данных) механизмов прогнозирования	Акцент на превентивное устранение возможных сбоев с применением средств предиктивной аналитики
Слабо развитые графические форматы предоставления информации («матрас аварий»)	Акцент на широкий спектр визуальных представлений и визуальную корреляцию информации
Закрытые решения	Широкое использование open source-библиотек, платформ, компонент

В-четвертых, сама возможность подобной динамической оптимизации появилась только после активного внедрения технологий виртуализации. Ранее применявшаяся модель «одно приложение — один физический сервер» предполагала только экстенсивное расширение, и то только в том случае, если архитектура программно-аппаратных комплексов это поддерживала. Теперь же, когда все базовые ресурсы в виде вычислительных мощностей, систем хранения и сетевого сегмента могут быть проквантованы и при необходимости динамически увеличены или сокращены точно под текущие потребности, управление мощностями превращается из бумажного процесса в полноценный элемент операционной аналитики.

В-пятых, для системного прогнозирования и моделирования ситуаций «что-если» в многоуровневых многокомпонентных информационных системах возникает потребность в объективных показателях, а значит — становится востребованным качественное математическое описание информационных систем, включая применение теории массового обслуживания, системной динамики, агентного и дискретно-событийного моделирования. Для конечных пользователей привлечение научной базы для обеспечения качественной работы прикладного ПО дает определенные гарантии по достижению победы над бесконечными «зависаниями» и необходимостью исполнять свои обязанности во внеурочное время в силу постоянных проблем с ИТ.

В автоматизации процесса управления мощностями в вышеописанной постановке ключевую роль будет играть система мониторинга. Но классические системы мониторинга далеки от реальных потребностей (таблица).

Современный мониторинг — это действительно большие данные. Даже простая численная оценка для отдельного малого филиала дает показатели, измеряемые миллионами или миллиардами единиц. Например, мониторинг 250 устройств дает следующие примерные оценки: 250 информационных устройств * 10 ресурсов на устройство * 3 метрики на ресурс * 2 измерения в минуту = 21 млн. измерений в сутки.

В настоящий момент сбор, хранение и обработка больших данных более не связаны с техническими

Сначала появляется мысль, затем эта мысль организуется в идеи и планы, затем происходит трансформация этих планов в реальность. Начало всегда в вашем воображении.
Наполеон Хилл

проблемами. В свете этого современные системы мониторинга фактически трансформируются в аналитические системы (Data Science) по контролю за ИТ-инфраструктурой (рис. 1). Инженеров, а уж тем более бизнес-заказчиков мало интересуют отдельные показатели или даже наборы показателей. Важно из всего потока информации вычленять только те метрики, измерения и записи, которые значимы с точки зрения влияния на бизнес-процессы и на безотказное и эффективное функционирование инфраструктуры. Эта задача как нельзя лучше соотносится с первоначальным назначением ЭВМ, а именно, цифровой обработкой данных.

При этой трансформации предполагается, что задача сбора данных и аварий за прошедшие 30 лет уже вышла на технологическое плато и ключевые проблемы смещаются именно в сторону обработки информации. В частности, для вычленения аномалий в задаче мониторинга активно используются различные подходы и методики из разных предметных областей, ядерной физики, биологии, теории очередей, цифровой обработки сигнала и пр., в том числе (но не ограничиваясь): контроль отклонений от адаптивного базового уровня (Adaptive baseline); поиск выбросов/исключительных значений (Outlier detection), в том числе на потоковых данных; фильтрация дребезга путем управления временем допустимого превышение порога (Time-over-threshold); прогнозирование и предиктивная аналитика (Predictive analytics); моделирование систем с использованием математического аппарата систем массового обслуживания (Queuing theory modeling); различные типы алгоритмов машинного обучения (Machine learning).

Далее, будучи ограниченными размерами статьи, тезисно затронем логическую цепочку между принимаемыми мерами и следствиями, а также выводами, которые из этих следствий проистекают. Все это в том или ином виде сейчас реализуется в системах мониторинга нового поколения.

В частности, разрабатываемый «Техносервом» продукт t.Mon опирается на большинство из указанных ниже подходов и следствий. Важным моментом является широкое использование open-source компонентов и открытость в части архитектуры, API, используемых алгоритмов и т. д.

Сбор данных, ключевые изменения

• Переход от событийной модели, когда система мониторинга пассивно получает аварийные сообщения от оборудования, к активному сбору данных с высокой частотой опроса оборудования и систем, хранения «сырых» данных, а также мультипротокольностью сбора данных.

• Допущение о «скорее» работоспособности, нежели о простое контролируемой системы (случай, когда время работы системы много больше времени простоев) вкупе с активным сбором данных дает большой набор маркированных почти равномерно распределенных измерений, что позволяет использовать в последующей обработке математический аппарат для работы с временными рядами (Time-Series, пары значений «временная метка — значение метрики»).

Работа с временными рядами. Следствие 1. Возможность формирования краткосрочных прогнозов (реализация механизма адаптивных порогов):

• высокая частота сбора метрик позволяет реализовать автоматическое формирование статистического базового профиля для значений метрик (адаптивные пороги);

• адаптивные базовые профили позволяют перейти от контроля превышения (выбросы в показателях) «жестких» ручных порогов к адаптивным, сократив число пропусков или ложных сигналов тревоги;

• заложенные в t.Mon алгоритмы позволяют проводить расчет адаптивных порогов для всех контролируемых метрик (десятки и сотни тысяч и более) в режиме, близком к реальному (зависит от предоставленных аппаратных мощностей). Большинство существующих западных решений имеют маркетинговую декларацию подобных возможностей, но при этом требуются большие, на несколько порядков аппаратные мощности, а методика расчета и корректность ее применения остается покрытой тайной;

• владение алгоритмом и его реализацией позволяет подстраивать его под специфику бизнеса, то есть специфичный ацикличный характер утилизации метрик в рамках отдельного внедрения.

Работа с временными рядами. Следствие 2. Возможность формирования долгосрочных прогнозов:

• появление данных, критически необходимых для постановки процесса управления мощностями;

• оптимизация и консолидация ИТ-ресурсов без потери качества в работе бизнес-процессов;

• повышение качества ИТ-сервисов и бизнес-процессов, оказываемых на этой инфраструктуре;

• раннее детектирование возможных сбоев, связанных с отказами оборудования («мигающих» неисправностей);

• своевременное и обоснованное планирование закупок оборудования (оптимизация закупочных цен).

Адаптивный порог. Следствие 1. Возможность построения адаптивного мониторинга за счет замыкания обратной связи:

• краткосрочное прогнозирование (отклонение от адаптивных порогов) позволяет решить задачу поиска компромисса между глубиной мониторинга и его полезностью:

– в нормальном состоянии информационной системы снимается минимум метрик с пониженной частотой опроса;

– при ожидании возникновения отклонений от нормы агенты сбора могут получать от ядра команды на изменение частоты сбора и объема собираемых метрик;

– при наличии информации о топологической связности объектов ядро может управлять глубиной мониторинга, в том числе и по топологическому дереву объектов/компонент.

Адаптивный порог. Следствие 2. Применение декларативной модели ИТ-сервисов.

При построении моделей ИТ сервисов возможны следующие подходы:

• декларативная модель — описание ИТ сервиса в терминах бизнеса без внутренней детализации («черный ящик»);

• императивная модель — детальное ресурсное описание внутренней структуры сервиса и правил взаимодействия ресурсов (ресурсно-сервисная модель).

Процесс управления уровнем качества сервиса (SLM) универсален для обеих моделей.

Каждый из этих подходов имеет свои плюсы и минусы, а также рекомендуемую область применения. Причем, как обычно, недостатки являются продолжением достоинств, которые легко понять на следующем примере.

В качестве простейшего образца можно использовать архитектуру типичного высоконагруженного трехзвенного приложения: АРМ пользователя — WAN — балансировщик — Web-сервер (ферма серверов) — сервер приложений (ферма серверов) — БД (кластер) + немного важных инженерных ресурсов. Все серверы работают в виртуальной среде с динамическим управлением ресурсами. Граф зависимости ресурсов принимает вид, похожий на развесистую структуру, подобную отраженной на рис. 2.

Классический ресурсно–сервисный подход:

– Требует создания CMDB (Configuration Management Data Base, ITIL) с детальным описанием компонентов ИТ-сервиса и их взаимодействием, что хорошо работает лишь для квазистатичных и простых по структуре ИТ-сервисов.

– В динамической многокомпонентной среде описание и поддержание в актуальном состоянии четких взаимосвязей становится крайне трудозатратным, если вообще возможным. Критерием возможности примем отношение скорости возникновения изменений в структуре ИТ сервиса к скорости процессной отработки по коррекции этих изменений в описывающих моделях.

– Жесткая ресурсно-сервисная модель не позволяет учитывать нюансы взаимодействия компонент. Все механизмы по приоритезации аварий и поиску первопричины работают строго в рамках модели. И нет никаких гарантий, что эта модель может быть усложнена, причем по многим причинам. В этом контексте выделим следующие ключевые проблемы: нестабильность сложной модели требует тщательной настройки правил распространения аварий и подстройки весовых коэффициентов по ребрам графа; элементарное незнание служб эксплуатации тонких, но важных деталей о внутренней структуре моделируемых сервисов; распадение зон ответственности с автоматическим вовлечением соответствующей бюрократической машины по согласованию взаимодействий различных подразделений, ответственных за работу ИТ сервиса.

– Ресурсно-сервисный подход применим по большей части только к поиску сбойных (отказавших), но не деградировавших по производительности элементов. Классические решения западных производителей реализуют в первую очередь event propagation, то есть восходящую передачу событий (или аварий) от ресурсов к ИТ-сервису. Вопросы производительности затрагиваются весьма косвенно, только путем формирования отдельной подсистемой управления производительностью аварийных сообщений по превышению контролируемыми метриками жестко установленных порогов.

Таким образом, простая и удобная идея (плюс) описания ИТ сервиса в виде графа ресурсов терпит фиаско на сложных ИТ-сервисах в виртуальной архитектуре, а также при попытках решить проблемы поиска деградации бизнес-операций (минус).

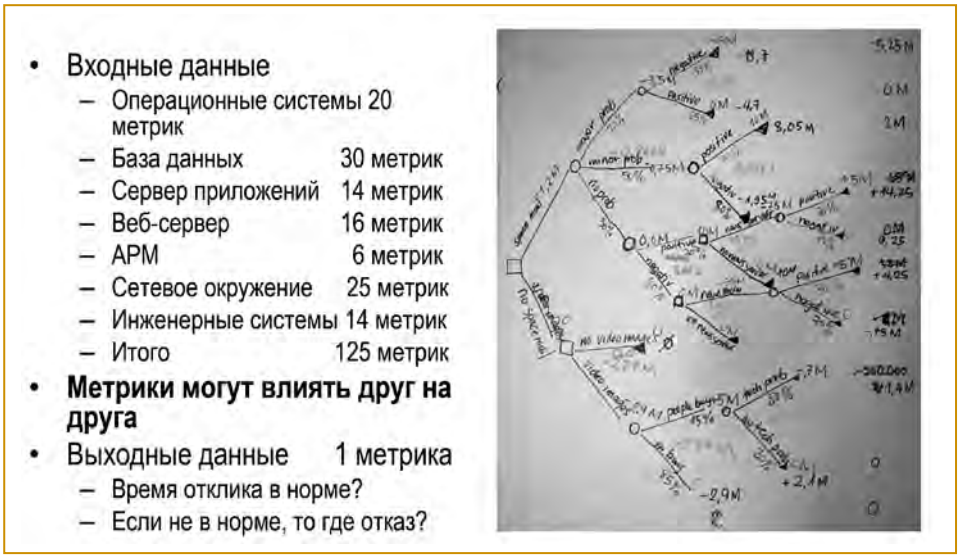

Рис. 2 Декларативная модель ИТ сервисов: когда ресурсно-сервисная модель слабо или вообще не применима

Декларативный подход позволяет обойти большую часть ограничений ресурсно-сервисного подхода по примерно следующему алгоритму, исполняемому в автоматизированном режиме:

– выбрать ресурсы (ручное задание);

– скомпоновать в сервис без четкого указания связей (ручное задание);

– накопить статистику по метрикам ресурсов (автоматизированный режим);

– применить элементы машинного обучения для формирования гипотез влияния технологических метрик ресурсов на бизнес-метрику, каковой является время отклика бизнес-операции (частично или полностью автоматизированный режим).

Декларативный подход применим как к обработке событий и аварий, так и к поиску деградировавших и сбойных элементов, повлиявших на деградацию ИТ-сервиса.

Переход к проактивному мониторингу, оперированию с временными рядами и адаптивными порогами позволяет существенно упростить и удешевить решение задачи поиска причин деградации в работе сложных программно-аппаратных комплексов (ИТ сервисов) без детального погружения во внутреннюю структуру этих комплексов.

Настоящая статья никоим образом не претендует на научное изыскание, а скорее является кратким обзором ожидаемых изменений в задаче мониторинга. Этим изменениям неизбежно способствует экспоненциальный рост числа «умных вещей», в частности, предметов домашнего обихода, связанных в сеть (Internet of Things, IoT), поскольку все это многообразие умных вещей работает по IP (многие через 3G/4G) и их необходимо контролировать, использовать их данные для прогнозирования, в т. ч. отказов и проблем, а также для доп. схем монетезации дополнительными адресными сервисами для владельцев «умных вещей», в том числе со стороны компаний-производителей. Мониторинг как сбор телеметрии + аналитика является ключевым кубиком в развитии IoT, а IoT изменяет требования к современным системам мониторинга.

Применительно к продукту t.Mon можно отметить, то в настоящий момент он пилотируется у нескольких заказчиков (промышленность, энергетика, ритейл, телеком, госструктуры), причем в совершенно различных гранях, органично вписывающихся в общую архитектуру. t.Mon пилотируется:

• как классическая EMS/NMS[2] система для программно-аппаратных комплексов;

• как система мониторинга бизнес-операций и здоровья Информационных систем;

• как система аналитических панелей визуализации, предоставляющих сводную оперативную информацию для дежурных смен и для бизнес-заказчиков;

• как система прогнозирования в задаче управления мощностями;

• как система мониторинга массового числа примитивных оконечных устройств (например, датчики и камеры в магазинах).

Тема «горячая», продукт находится в активном функциональном расширении в соответствии с озвученными выше трендами, потребностями и планами. Работает по nix операционной системой, типичные инсталляции проводятся либо в виртуальном окружении, либо на серверном оборудовании общего пользования x64 архитектуры. Нескольких таких серверов достаточно для постановки на мониторинг оконечного оборудования целого предприятия. Потребные же объемы дискового пространства определяются простой математикой: частота сбора * число метрик * глубина хранения.

Тренды на «поумнение машин», в том числе с применением элементов искусственного интеллекта для решения бизнес и технологических задач, озвученные Gartner в отчете «Top 10 Strategic Technology Trends for 2016: At a Glance» (http://www.gartner.com/smarterwithgartner/top-ten-technology-trends-signal-the-digital-mesh/) применимы и к промышленному сектору, в том числе ИТ в промышленности.

Цифровая трансформация неизбежна, это вопрос только времени. Мониторинг как объединение сбора телеметрии и интеллектуальной автоматизированной надстройки (центр аналитики и принятия операционных решений) позволяют построить замкнутый контур и тем самым вывести процесс эксплуатации ИТ и информационных систем на уровень, адекватный внутренней сложности контролируемых систем и вызовам со стороны современной программной инженерии.

Список литературы

1. *Соболев А.Ю., Шипулин А.С.* Мониторинг активности в промышленных системах и сетях как безопасный подход к борьбе с киберугрозами // Автоматизация в промышленности. 2015. №2.
2. *Батов И.И., Переведенцев А.В.* ИТ-инфраструктура предприятия: особенности, тренды, опасности в кризис и не только // Автоматизация в промышленности. 2015. №2.

Шутов Илья Владимирович *– канд. физ.-мат. наук, начальник отдела OSS/ITSM продажи решений компании Техносерв.*
Контактный телефон (495) 648-0808.
E-mail: info@technoserv.com

[2] Element management system (EMS) — ПО, предназначенное для управления и контроля отдельного сетевого элемента группы однотипных элементов. Network Management System (NMS) – система управления сетью.