УДК 004.052.2

М.Г. Дубровин, И.Н. Глухих

МОДЕЛИ И МЕТОДЫ ПРОАКТИВНОГО МОНИТОРИНГА ИТ-СИСТЕМ

ФГАОУ ВО «Тюменский государственный университет», Тюмень, Россия

Высокая стоимость ИТ-систем организаций и значительные потери от незапланированных простоев, вызванных сбоями в подобных системах, обуславливают актуальность поиска новых подходов к мониторингу. Наиболее совершенным является проактивный подход к мониторингу, который направлен не только на регулярную проверку состояния объектов мониторинга и реагирование на инциденты, но и на прогнозирование возможных аварийных ситуаций на ранней стадии. Данная статья направлена на исследование моделей и методов проактивного мониторинга ИТ-систем. Основная задача проактивного мониторинга сводится к задаче прогнозирования временных рядов с учетом внешних факторов. Для раскрытия исследуемого процесса рассмотрена классификация моделей прогнозирования временных рядов и произведен обзор современных работ, посвященных моделям и методам прогнозирования работоспособности различных компонентов ИТ-инфраструктуры. Проведенный анализ показал, что не существует обобщенной модели, позволяющей решать любую поставленную задачу прогнозирования состояния ИТ-систем. Процесс реализации модели и соответствующего метода должен базироваться на возможностях выбранных классов моделей и требованиях к решению задачи. В процессе обзора сформулирован ряд предложений, которые позволят повысить эффективность проактивного мониторинга и качество модели прогнозирования. Проведение комплексного мониторинга компонентов ИТ-системы позволяет проанализировать корневые причины, которые приводят к неработоспособному состоянию системы. Для корректного выявления пороговых значений работоспособного состояния объектов необходимо использовать «динамические пороги». Прогнозирование состояния объектов мониторинга на несколько шагов вперед является актуальным вопросом для распределенной ИТ-системы.

Ключевые слова: проактивный мониторинг, модель прогнозирования, ИТ-система.

Введение

В настоящее время практически все современные организации для автоматизации выполнения бизнес-процессов или процессов деятельности используют информационные технологии (ИТ) различной сложности, которые разворачиваются на основе ИТ-системы, включающей в себя разнообразные информационные и телекоммуникационные ресурсы. Высокая стоимость ИТ-систем и значительные потери от простоев, вызванных сбоями в ИТ-системах, обуславливают актуальность повышения надежности функционирования ИТ-инфраструктуры предприятия. Для обеспечения работоспособности ИТ-системы

применяются различные автоматизированные системы мониторинга, заключающиеся в постоянном наблюдении и периодическом анализе объектов системы, с отслеживанием динамики происходящих с ними изменений.

В мониторинге состояния ИТ-систем различают два подхода к обнаружению и управлению изменениями – реактивный и проактивный [12].

При реактивном мониторинге система получает информацию о состоянии компонентов ИТ-системы в режиме реального времени. Это позволяет реагировать на множество аварийных ситуаций, которые могут прогрессировать в ИТ-системе. Аварийные ситуации обычно говорят о неисправности в сети или означают аномальное поведение компонентов ИТ-системы, которое может привести к неисправности. Системы реактивного мониторинга позволяют определять только часть проблем в сложных ИТ-системах, испытывая затруднения при анализе функционирования сложных распределенных приложений [5]. При этом диагностика и локализация ошибок в ИТ-системах производится после обнаружения неполадок, так же, как и определяются только проблемы, уже существующие в аппаратном или программном обеспечении.

Более совершенными являются средства проактивного мониторинга, которые не только обеспечивают дистанционный мониторинг в режиме реального времени, регулярные проверки исправности компонентов ИТ-системы, но и позволяют прогнозировать критические состояния системы и на ранней стадии, а так же генерировать предупреждения об ошибках, для того, чтобы предотвратить возникновение отказов в работе ИТ-системы [5]. Такой мониторинг позволяет анализировать работоспособность распределенных многоуровневых приложений. Главным отличием этих систем от реактивных является понимание логики распределенных приложений, а также способность предсказывать на основе анализа накопленных данных возможные сценарии развития текущей ситуации. За счет этого системы проактивного мониторинга могут выявлять и предсказать гораздо больше проблем в ИТ-системе, что позволяет устранять неполадки еще на этапе их зарождения и развития. Системы такого типа позволяют не только выявить конкретный некорректно работающий в данный момент аппаратный или программный элемент ИТ-системы, но и предсказать возможность отказа этого элемента в будущем, за счет чего обеспечивается более стабильная работа ИТ-системы, и минимизируются издержки, вызванные с ее простоем.

Модели и методы проактивного мониторинга

Основная задача системы проактивного мониторинга сводится к задаче построения точного прогноза дальнейшего состояния компонентов ИТ-системы. Развитие процессов, которые необходимо предсказывать,

описываются временными рядами. Временной ряд представлен последовательностью значений некоторых величин, для которых известен момент времени, в который они были получены [2]. При прогнозировании временного ряда требуется определить функциональную зависимость, адекватно описывающую временной ряд. Для корректного прогнозирования состояния ИТ-системы, необходимо использовать не только фактические значения исследуемого ряда, но и значения набора внешних факторов, влияющие в определенной мере на формирование прогноза. Внешними факторами, например, могут служить: время, день недели, рабочий/выходной/праздничный день. Такие признаки могут быть использованы в качестве внешних факторов, поскольку известно их значение в момент прогноза, а значит, возможно учесть эти значения в модели прогнозирования. Цель создания модели прогнозирования состояния ИТ-системы организации состоит в получении такой модели, которая позволяет наиболее точным образом отображать дальнейшее поведение исследуемого объекта.

Пусть значения временного ряда, представляющие перечень показателей работоспособности ИТ-системы известны в дискретные моменты времени $t = 1,2,\dots,T$. Обозначим временной ряд $Z(t) = Z(1),Z(2),\dots,Z(t)$. В момент времени T необходимо определить значения процесса $Z(t)$ в моменты времени $T+1,\dots,\ T+P$. Момент времени T называют моментом прогноза, а величину P – временем упреждения [2]. Обозначим временной ряд внешних факторов как $X(t)$. Пусть каждый внешний фактор $X_i(t)$ доступен в моменты времени $t_i = 1,2,\dots,T$. Будем считать также, что временные ряды внешних факторов и основной временной ряд приведены к единой шкале времени t. В момент прогноза T необходимо определить будущие значения исходного процесса $Z(t)$ в моменты времени $T+1,\dots,T+P$, принимая во внимание влияние внешних факторов $X_1(t),\dots,X_s(t)$. Для получения значений временного ряда в будущие моменты требуется определить функциональную зависимость, отражающую связь между прошлыми значениями $Z(t)$ и будущими, принимая во внимание влияние на исходный временной ряд внешних факторов $X_1(t),\dots,X_s(t)$ и случайной ошибки ε_t:

$$Z(t) = F(Z(t-1),Z(t-2),\dots,X_1(t-1),X_1(t-2),\dots,X_s(t-1),X_s(t-2),\dots) + \varepsilon_t$$

.

Такая зависимость называется моделью прогнозирования с учётом внешних факторов $X_1(t),\ \dots,X_s(t)$. [9]

Соответственно, требуется разработать такую модель и соответствующий ей метод прогнозирования работоспособности ИТ-

системы, для которых среднее абсолютное отклонение истинного значения $Z(t)$ от прогнозируемого

$$\bar{Z}(t) = F(Z(t-1), Z(t-2), \dots, X_1(t-1), X_1(t-2), \dots, X_s(t-1), X_s(t-2), \dots)$$

стремится к минимальному для заданного времени упреждения P:

$$\bar{\mathrm{E}}(t) = \frac{1}{P}\sum_{i=T}^{T+P} |\bar{Z}(t) - Z(t)| \to min\,.$$

Существует множество моделей и соответствующих им методов прогнозирования, на данный момент насчитывается свыше 100 классов моделей прогнозирования [6]. В работах [6,9] известные модели и методы прогнозирования делятся на два класса: интуитивные и формализованные. Интуитивные методы прогнозирования применяются, если объект прогнозирования прост и хорошо изучен, либо настолько сложен, что учесть влияние внешних воздействий при помощи аналитических подходов невозможно. По своей природе интуитивные методы основываются на задействовании профессионального опыта и интуиции исследователя. Эти методы используются для анализа процессов, течение которых либо полностью, либо частично не может быть математически формализовано.

Формализованные методы – это методы прогнозирования, в результате которых строятся модели прогнозирования, то есть определяют такую математическую зависимость, которая позволяет вычислить будущее значение процесса, то есть сделать прогноз [9]. Модели временных рядов относятся к классу формализованных методов. В свою очередь, модели временных рядов разделяются на статистические и структурные модели. В статистических моделях функциональная зависимость между будущими и фактическими значениями временного ряда, а также внешними факторами задана аналитически. К статистическим моделям относятся следующие группы [9]:

- регрессионные модели;
- авторегрессионные модели;
- модели экспоненциального сглаживания.

В структурных моделях функциональная зависимость между будущими и фактическими значениями временного ряда, а также внешними факторами задана структурно. К структурным моделям относятся следующие группы [9]:

- нейросетевые модели;
- модели на базе цепей Маркова;
- модели на базе классификационно-регрессионных деревьев.

Предложено множество моделей, и соответствующим им методам прогнозирования временных рядов, применимых к задачам

прогнозирования состояния ИТ-инфраструктуры. Часть методов представляет собой вариации и комбинации нескольких методов с различными усовершенствованиями.

Распространенными являются работы, в которых рассматривается прогнозирование локальных и корпоративных интернет-сетей. Предлагается использование алгоритма прогнозирования Хольта-Винтерса для прогнозирования неисправностей в локальных сетях. Экспоненциальное сглаживание обеспечивает наглядное представление о тренде и позволяет делать краткосрочные прогнозы. Отличие от экспоненциального сглаживания заключается в способности метода обнаруживать тренды, относящиеся к коротким периодам в моменты времени, непосредственно предшествующие прогнозным, и экстраполировать эти тренды на будущее [10]. В другой работе рассматривается использование гибридных нейронных сетей для прогнозирования состояния компьютерных сетей. В рассматриваемой модели объединены три искусственные нейронные сети: самоорганизующаяся карта Кохонена, трехслойная гибридная нейронная сеть и многослойный перцептрон [4].

Рассматриваемые модели применяются также в задачах прогнозирования потенциальных проблем и выполнения корректирующих действий в крупных кластерных системах. Для прогнозирования критических ситуаций в кластерных системах представлена модель, использующая комбинацию методов интеллектуального анализа данных и Байесовских сетей [14]. Для повышения отказоустойчивости кластерных установок рассмотрена модель, основанная на построении аппроксимирующей функции по методу наименьших квадратов [1].

Модели и методы прогнозирования применяются для идентификации дальнейшего состояния серверных компьютерных систем. Для мониторинга и оценки состояния вычислительных центров предложено использование нейронной сети, позволяющей прогнозировать поведение системы на несколько шагов вперед. Система мониторинга способна подстраиваться под изменения в структуре вычислительного центра, обеспечивая гибкую оценку состояния, что позволяет убрать ложные сообщения об ошибках в работе вычислительного центра [3]. В следующей работе предложен метод прогноза производительности серверных систем, так же основанный на нейронных сетях. Отличительной особенностью является создание нечеткой нейросетевой модели прогноза производительности, которая отличается тем, что, используя формализацию знаний в виде нечетких правил, позволяет анализировать систему факторов и дает комплексную оценку производительности, что упрощает взаимодействие человека с компьютерной системой и уменьшает вероятность неправильного прогноза [8].

Далее рассмотрено использование методов прогнозирования по отношению к состоянию баз данных и системам управления базами данных (СУБД). В статье рассматривается использование метода с использованием нейронной сети для повышения дальнейшей производительности показателей СУБД. Предложенная система не учитывает резкие скачки в рабочей нагрузке, правильность алгоритма зависит от правильно выбранного учебного набора данных [13]. В другой статье предлагается методика прогнозирования развития и масштабирования СУБД Oracle, построенная на основе теории массового обслуживания. Методика позволяет спрогнозировать приближение точки краха системы (бесконечного времени обработки запроса), определить проблемные подсистемы (процессорная подсистема или подсистема ввода/вывода), сделать прогноз потенциальной масштабируемости. В качестве математической модели рассмотрена модель Эрланга - С (система массового обслуживания с очередями) в нотации статистик СУБД Oracle [7].

Проанализированные работы рассматривают вопросы мониторинга и прогнозирования состояния отдельных составляющих ИТ-системы. Подобные системы, направленные на отслеживание отдельных компонентов в изоляции, не учитывают состояние других подсистем ИТ-системы, влияющих на её общее состояние. Наличие комплексного мониторинга и правильное понимание того, какова должна быть работоспособность на уровне каждого компонента, позволяет проанализировать корневые причины (Root Cause Analysis) возможного неработоспособного состояния системы. Анализ корневых причин – это метод устранения неполадок, основанный на том, что наиболее эффективным способом решения проблемы и предотвращения ее повторения является определение ее основной причины и принятие мер по ее устранению. **Root Cause Analysis (RCA) по существу является реактивным методом.** Это означает, что с учетом проблемы или события процедуры **RCA** начинают выявлять первопричины, чтобы предотвратить повторение одной и той же проблемы. **Однако после реализации и с постоянным выполнением RCA преобразуется в метод прогнозирования проблем [11].**

В процессе мониторинга объектов ИТ-систем значения контролируемых параметров регистрируются через определенные промежутки времени и образуют систему взаимосвязанных временных рядов. Фиксируемые параметры описываются выбранной математической моделью, используемой в дальнейшем для прогнозирования значений соответствующих характеристик. Обработанные данные сравниваются с заложенными пороговыми значениями метрик, и производится статистический анализ, корреляция и классификация полученных данных

исходя из заданной модели. Использование статичных пороговых значений для метрик не является корректным. К примеру, для одних объектов мониторинга одинакового типа такая метрика, как загрузка центрального процессора на 85% процентов будет считаться нормальным состоянием работы, а для других аварийным. Аналогию можно провести со временем замера значений метрик. Исходя из бизнес–процессов многих организаций, 85% используемой физической памяти сервера в дневное время может считаться нормальным состоянием, тогда как в ночное время использование такого количества памяти является критической ситуацией. Исходя из этого, система проактивного мониторинга должна уметь анализировать исторические данные, изучать поведение объектов и на основании этого строить так называемые «динамические пороги» для каждого отдельного объекта мониторинга. То есть система мониторинга должна «обучаться» и понимать, что является нормальным подведением объекта, а что сигнализирует об аварии.

Многие современные системы мониторинга позволяют прогнозировать изменение исследуемых объектов на один шаг вперед, т.е обеспечивают реагирование на определенное событие. В рамках прогнозирования состояния распределенной ИТ-системы этого может быть недостаточно. Рассмотрим распределенную инфраструктуру, которая включает несколько объектов, отвечающих за определенный сервис. При выходе из строя одного из объектов, нагрузка в системе распределится на оставшиеся узлы. Система прогнозирования, способная предвидеть поведение системы на один шаг, некорректно продиагностирует рассмотренную ситуацию. Система способна предвидеть отказ одного из узлов, но не способна спрогнозировать последующую нагрузку оставшихся работоспособных объектов. Исходя из этого, повышенная нагрузка оставшихся узлов может быть воспринята как критическая, хотя на самом деле является нормальным отражением рассмотренной ситуации. В свою очередь, ложные сообщения могут скрыть реальные сбои в работе ИТ-системы, что может привести к более тяжелым последствиям как для всей системы в целом, так и для сервиса в частности. Исходя из проведенного анализа можно сделать вывод, что для корректной оценки распределенной ИТ-системы, актуальным вопросом является создание системы проактивного мониторинга, способной гибко оценивать работоспособность ИТ-системы и прогнозировать события на несколько шагов вперед.

Заключение

В работе рассмотрена актуальность применения проактивного мониторинга для управления ИТ-системами, описаны преимущества над реактивным подходом к мониторингу. Поставлена основная задача проактивного мониторинга, заключающаяся в прогнозировании будущего состояния ИТ-системы. Рассмотрена классификация существующих моделей прогнозирования. Произведен анализ работ, посвященных существующим методам и моделям прогнозирования состояния различных компонентов ИТ-систем. Рассмотренные методы представляют собой вариации и комбинации нескольких других существующих методов с различными усовершенствованиями. Анализ работ показал, что не существует обобщенной модели, позволяющей решать любую поставленную задачу прогнозирования. Процесс реализации модели должен базироваться на возможностях выбранных классов моделей и требованиях к решению поставленной задачи. В процессе анализа сформулированы некоторые предложения, которые могут быть использованы для реализации концептуальной модели проактивного мониторинга и модели прогнозирования.

ЛИТЕРАТУРА

1. Ардентов А. А., Московский А. А., Первин А. Ю., Стоцкий М. В. Алгоритмы прогнозирования аппаратных сбоев в системе мониторинга кластерных установок // XII научно-практическая конференция университета города Переславля. – 2008. № 6 – С. 84-95.
2. Бокс Дж., Анализ временных рядов, прогноз и управление. / Дж. Бокс. Г.М.Дженкинс. – М.: Мир, 1974. – 406 с.
3. Петраков В. А., Богачев Д. Н. Применение нейронных сетей в мониторинге вычислительных центров // Известия Южного федерального университета. Технические науки. – 2009. № 2. С. 82-87.
4. Саенко И. Б., Скорик Ф. А., Котенко И. В. Мониторинг и прогнозирование состояния компьютерных сетей на основе применения гибридных нейронных сетей //Известия высших учебных заведений. Приборостроение. – 2016. – Т. 59. – №. 10.
5. Ролик А.И., Тимофеева Ю.С., Турский Н.И. Управление устранением неисправностей в ИТ-системах // Вестник НТУУ «КПИ». Информатика, управление и вычислительная техника. – 2008. № 49. С. 95-108.
6. Тихонов, Э.Е. Прогнозирование в условиях рынка. / Э.Е. Тихонов. – Невинномысск, 2006. – 221 с.

7. Трухачев А.А., Ивкина Е.А. Применение методики прогнозирования масштабируемости для построения систем высокой доступности на основе СУБД Oracle // Спецтехника и связь. 2011. №6.
8. Федоров Е. Е., Аль-Абабнех Х. А., Альрабаба Х. Метод прогноза производительности серверных компьютерных систем //Наукові праці Донецького національного технічного університету. Серія: Інформатика, кібернетика та обчислювальна техніка. – 2015. – №. 1. – С. 52-58.
9. Чучуева И. А. Модель прогнозирования временных рядов по выборке максимального подобия //Москва. – 2012.
10. Шелупанов А.А., Исхаков С.Ю., Тимченко С.В. Прогнозирование в системе мониторинга локальных сетей // Доклады Томского государственного университета систем управления и радиоэлектроники– 2012. № 1-2 – С. 100-103.
11. Alexander La rosa. Root Cause Analysis and Monitoring Tools: A Perfect Match. [Электронный ресурс] – Режим доступа: URL: https://blog.pandorafms.org/root-cause-analysis/ (Дата обращения: 24.01.2018)
12. Kothamasu R., Huang S. H., VerDuin W. H. System health monitoring and prognostics—a review of current paradigms and practices //The International Journal of Advanced Manufacturing Technology. – 2006. – Т. 28. – №. 9-10. – С. 1012-1024.
13. Rodd S. F., Kulkarni U. P. Adaptive tuning algorithm for performance tuning of database management system //arXiv preprint arXiv:1005.0972. – 2010.
14. Sahoo R. K. et al. Critical event prediction for proactive management in large-scale computer clusters //Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining. – ACM, 2003. – С. 426-435.

M.G. Dubrovin, I.N. Gluhih

MODELS AND METHODS OF PROACTIVE MONITORING OF IT-SYSTEMS

Tyumen State University,
Tyumen, Russia

The high cost of organizations' IT systems and the significant losses from unplanned downtime caused by failures in such systems, make the search for new approaches to monitoring urgent. The most advanced is the proactive approach to monitoring, which is aimed not only at regular monitoring of the status of monitoring objects and responding to incidents, but also in forecasting possible emergencies at an early stage. This article is aimed

at researching models and methods for proactive monitoring of IT systems. The main task of proactive monitoring is reduced to the task of forecasting time series taking into account external factors. To disclose the process under investigation, the classification of forecasting models of time series is considered and an overview of modern works devoted to models and methods for predicting the health of various components of the IT infrastructure is reviewed. The analysis showed that there is no generalized model that allows to solve any given task of forecasting the state of IT systems. The process of implementing the model and the corresponding method should be based on the capabilities of the selected classes of models and the requirements for solving the problem. During the review, a number of proposals are formulated that will improve the effectiveness of proactive monitoring and the quality of the forecast model. Conducting a comprehensive monitoring of the components of the IT system allows you to analyze the root causes that lead to an inoperative state of the system. For the correct detection of threshold values of the operable state of objects, it is necessary to use "dynamic thresholds". Forecasting the state of monitoring objects a few steps forward is an urgent issue for a distributed IT system.

Keywords: proactive monitoring, forecasting model, IT system

REFERENCES

1. Ardentov A. A., Moskovskiy A. A., Pervin A. Yu., Stotskiy M. V. Algoritmy prognozirovaniya apparatnykh sboev v sisteme monitoringa klasternykh ustanovok // XII nauchno-prakticheskaya konferentsiya universiteta goroda Pereslavlya. – 2008. No. 6 – pp. 84-95.
2. Boks Dzh., Analiz vremennykh ryadov, prognoz i upravlenie. / Dzh. Boks. G.M.Dzhenkins. – M.: Mir, 1974. – 406 p.
3. Petrakov V. A., Bogachev D. N. Primenenie neyronnykh setey v monitoringe vychislitel'nykh tsentrov // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. – 2009. No. 2. pp. 82-87.
4. Saenko I. B., Skorik F. A., Kotenko I. V. Monitoring i prognozirovanie sostoyaniya komp'yuternykh setey na osnove primeneniya gibridnykh neyronnykh setey //Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie. – 2016. – Vol. 59. – No. 10.
5. Rolik A.I., Timofeeva Yu.S., Turskiy N.I. Upravlenie ustraneniem neispravnostey v IT-sistemakh // Vestnik NTUU «KPI». Informatika, upravlenie i vychislitel'naya tekhnika. – 2008. No. 49. pp. 95-108.
6. Tikhonov, E.E. Prognozirovanie v usloviyakh rynka. / E.E. Tikhonov. – Nevinnomyssk, 2006. – 221 p.
7. Trukhachev A.A., Ivkina E.A. Primenenie metodiki prognozirovaniya masshtabiruemosti dlya postroeniya sistem vysokoy dostupnosti na osnove SUBD Oracle // Spetstekhnika i svyaz'. 2011. No.6.
8. Fedorov E. E., Al'-Ababnekh Kh. A., Al'rababa Kh. Metod prognoza proizvoditel'nosti servernykh komp'yuternykh sistem //Naukovi pratsi Donets'kogo natsional'nogo tekhnichnogo universitetu. Seriya: Informatika, kibernetika ta obchislyuval'na tekhnika. – 2015. – No. 1. – pp. 52-58.

9. Chuchueva I. A. Model' prognozirovaniya vremennykh ryadov po vyborke maksimal'nogo podobiya //Moskva. – 2012.
10. Shelupanov A.A., Iskhakov S.Yu., Timchenko S.V. Prognozirovanie v sisteme monitoringa lokal'nykh setey // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki– 2012. No. 1-2 – pp. 100-103.
11. Alexander La rosa. Root Cause Analysis and Monitoring Tools: A Perfect Match. [Elektronnyy resurs] – Rezhim dostupa: URL: https://blog.pandorafms.org/root-cause-analysis/ (Data obrashcheniya: 24.01.2018)
12. Kothamasu R., Huang S. H., VerDuin W. H. System health monitoring and prognostics—a review of current paradigms and practices //The International Journal of Advanced Manufacturing Technology. – 2006. – Vol. 28. – No. 9-10. – pp. 1012-1024.
13. Rodd S. F., Kulkarni U. P. Adaptive tuning algorithm for performance tuning of database management system //arXiv preprint arXiv:1005.0972. – 2010.
14. Sahoo R. K. et al. Critical event prediction for proactive management in large-scale computer clusters //Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining. – ACM, 2003. – pp. 426-435.