**КОМПЬЮТЕРНЫЕ ИССЛЕДОВАНИЯ**
**И МОДЕЛИРОВАНИЕ 2012 Т. 4 № 3 С. 661–668**

Ки&М

**ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ**

УДК: 004.75

# Методика оценки эффективности систем мониторинга вычислительных ресурсов

**П. В. Дмитриенко**

Объединенный институт ядерных исследований, Лаборатория информационных технологий,
Россия, 141980, Московская область, г. Дубна, ул. Жолио-Кюри, д. 6

E-mail: pauldmitrienko@gmail.com

*Получено 6 августа 2012 г.*

В данной статье рассмотрен вклад, вносимый системой мониторинга вычислительных ресурсов в работу распределенной вычислительной системы, и предложена методика оценки этого вклада и эффективности работы системы мониторинга на основе меры определенности состояния подконтрольной системы. Рассмотрено применение этой методики в ходе разработки и развития системы локального мониторинга Центрального информационно-вычислительного комплекса Объединенного института ядерных исследований.

Ключевые слова: мониторинг вычислительных ресурсов, системы управления, эффективность системы мониторинга

# Methods of evaluating the effectiveness of systems for computing resources monitoring

**P. V. Dmitrienko**

*Joint institute for nuclear research, Laboratory of information technologies, 6 Joliot-Curie st., Dubna, Moscow region, 141980, Russia*

**Abstract.** – This article discusses the contribution of computing resources monitoring system to the work of a distributed computing system. Method of evaluation of this contribution and performance monitoring system based on measures of certainty the state-controlled system is proposed. The application of this methodology in the design and development of local monitoring of the Central Information and Computing Complex, Joint Institute for Nuclear Research is listed.

Keywords: monitoring of computing resources, management system, performance of monitoring systems

Citation: *Computer Research and Modeling*, 2012, vol. 4, no. 3, pp. 661–668 (Russian).

Ключевым элементом в обеспечении бесперебойной работы любой сложной распределенной вычислительной системы является качественная система мониторинга (СМ). Данные, предоставляемые средствами мониторинга, имеют большое значение как для системных администраторов, ответственных за предоставление оборудования и каналов, так и для потребителей предоставляемых системой ресурсов и служб, желающих оценить эффективность его работы. Помимо получения общего представления о работе и текущем состоянии системы, а также своевременного реагирования на нештатные ситуации, эти данные могут быть использованы для исследования закономерностей и взаимосвязей между объектами мониторинга с целью оптимизации и повышения эффективности их работы. Однако не менее важной задачей является оценка эффективности работы самих средств мониторинга и вклада, вносимого ими в работу системы. Представляется важным разработка критериев, понятийного и математического аппарата, применимых для решения этой проблемы.

Естественно для этой цели использовать методы системного анализа, а также и теории управления, так как задача, которую призвана решать система мониторинга, является составной частью основной задачи управления системой в ее традиционной формулировке. Требуется найти (осуществить) такое управляющее воздействие, при котором для ряда заданных характеристик (критериев) подконтрольной системы $J_i i = 1 \ldots n$ выполняется определенный набор требований [Астахов и др., 2012]. Например, нахождение критерия в допустимой области изменения, прохождение траектории процесса через заданные точки и т. п.

В задаче мониторинга всегда можно выделить две взаимодействующие системы: *подконтрольную систему*, для эффективного управления которой применяются средства мониторинга; и *систему мониторинга*, объединяющую эти средства. *Объект мониторинга* – это элемент подконтрольной системы (для вычислительного комплекса – устройство либо служба), за состоянием которого (характеризующимся набором свойств) осуществляется регулярное наблюдение с целью управления, анализа протекающих с его участием процессов, выявления и прогнозирования нештатных состояний. *Нештатное (кризисное) состояние* объекта мониторинга (в отличие от *стабильного*) – состояние, препятствующее корректной работе системы, над которой осуществляется контроль; *нештатная ситуация* – ситуация нахождения одного или более элементов системы (объектов мониторинга) в нештатном состоянии. *Событие* в системе мониторинга – более широкий термин, обозначающий любое значимое для наблюдателя изменение состояния одного или нескольких объектов мониторинга.

Применение системного анализа, в частности метода функциональной декомпозиции, позволяет выделить следующие составные части, могущие входить в состав любой СМ [Коренько в, Дмитриенко, 2011].

1) *Подсистема сбора данных* – осуществляет опрос объектов мониторинга с заданными временными интервалами для получения значений исследуемых параметров этих объектов.

2) *Подсистема хранения* – отвечает за накопление, хранение, архивацию данных о результатах проверок. Включает компоненты для работы с базами данных (БД) или иными репозиториями.

3) *Подсистема анализа данных* – включает компоненты, производящие исследования данных, накопленных системой, их статистический анализ и тому подобные операции.

4) *Подсистема оповещения* – отвечает за уведомление ответственных лиц о событиях СМ.

5) *Подсистема вывода* – отвечает за представление информации о работе системы и состоянии объектов в виде удобном для восприятия пользователя.

6) *Подсистема коррекции* – предоставляет возможность выполнения системой действий по устранению возникших нештатных ситуаций.

Некоторые из этих подсистем могут и не присутствовать в конкретной рассматриваемой СМ. Система же, в которой реализованы все эти подсистемы, приближается по функциональным свойствам к классической системе автоматического управления (САУ), где элементы подсистемы сбора данных выступают в качестве измерительных устройств, а элементы подсистемы коррекции – в качестве исполнительных. Роль, отводимую устройству управления, исполняют элементы подсистем анализа данных и коррекции.

Рассмотрим для простоты систему мониторинга (СМ), реагирующую на обнаруженные нештатные ситуации только одним способом: генерацией диагностического сообщения. Задача такой системы сводится исключительно к выявлению и максимальной локализации нештатных ситуаций в подконтрольной системе, а также предоставлению максимально полной информации о ее функционировании; иначе говоря – к снижению меры неопределенности технического состояния (ТС) подконтрольной системы. Данные, вырабатываемые такой системой, передаются либо САУ, либо человеку-оператору, которые на их основе осуществляют управляющие воздействия.

Модель взаимодействия такой системы мониторинга с подконтрольной системой можно описать в виде

$$M = \langle O,\ P, f_p,\ D_o,\ D_p,\ S, f_u \rangle,$$

где $O$ – множество объектов подконтрольной системы, $P$ – множество свойств, характерных для объектов подконтрольной системы, $f_p$ – функция принадлежности, определяющая наличие или отсутствие того или иного свойства у некоторого объекта:

$$f_c = O \otimes P \to \{0,1\},$$

$D_o$ – множество упорядоченных пар объектов, обозначающих наличие зависимости стабильного состояния второго объекта пары от стабильного состояния первого; $D_p$ – множество упорядоченных четверок $\langle o_1, p_1, o_2, p_2 \rangle$, обозначающих наличие зависимости стабильного состояния свойства $p_2$ объекта $o_2$ от стабильного состояния свойства $p_1$ объекта $o_1$. $S$ – множество сенсоров (или методов проверок) системы мониторинга; $f_u$ – функция применимости, определяющая возможность использования данного сенсора (метода) для контроля состояния некоторого свойства:

$$f_u = S \otimes P \to \{0,1\}.$$

Мера определенности технического состояния подконтрольной системы может быть представлена как

$$D = \frac{\sum_{i=1}^{c} w_{p_i} n_{p_i}}{\sum_{j=1}^{d} w_{p_j} n_{p_j}}, \qquad (1)$$

где $p_i$ – свойства объектов, охваченные системой мониторинга (т. е. те, для которых существует хотя бы один $c\, f_u(p_i, s) = 1$); $p_j$ – все свойства объектов подконтрольной системы (т. е. те, для которых существует хотя бы один $cf_p(o, p_i) = 1$); $w$ – вклад свойства в функционирование подконтрольной системы; $n_p$ – число объектов, обладающих свойством $p$ в подконтрольной системе.

Очевидно, что $D$ не может быть больше 1 и принимает это значение при выполнении следующего условия:

$$\forall p \in P \exists s \in S, f_u(p, s) = 1,$$

то есть для каждого из свойств, определяющих техническое состояние подконтрольной системы, в СМ существует хотя бы один метод мониторинга, применимый для контроля над состоянием этого свойства.

На практике, однако, различные СМ, обладающие указанным свойством полного охвата подконтрольной системы, различаются по степени полноты предоставляемой ими информации. В реальных системах мониторинга различные диагностические сообщения обладают разной

информативностью, позволяя с большей или меньшей точностью локализовать объект или его свойство, служащие источником нештатной ситуации. Сообщения, а значит, и порождающие их сенсоры (методы) системы мониторинга могут предоставлять разное количество дополнительных данных о состоянии объекта, важных для принятия решения об управляющем воздействии.

Нами был осуществлен анализ данных, накопленных за время разработки и внедрения системы локального мониторинга (СЛМ) центрального информационно-вычислительного комплекса (ЦИВК) ОИЯИ, который является крупнейшим в России комплексом для моделирования, хранения, обработки и анализа данных с экспериментов на Большом адронном коллайдере (LHC). За 2011 год на его базе было выполнено около 6 миллионов пользовательских задач, предоставлено около 27 миллионов часов процессорного времени и около 1 Петабайта дискового хранилища. Этот комплекс активно используется для крупномасштабных вычислений многими научными коллективами ОИЯИ, России и других стран [Кореньков, Дмитриенко, 2011]. Системы хранения данных вычислительного комплекса широко используются для поддержки проектов ОИЯИ и международных коллабораций, в том числе проекта NICA/MPD. Ресурсы ЦИВК ОИЯИ по состоянию на март 2012 года включают в себя 2072 вычислительных узла, более 80 управляющих серверов, базовая операционная система, под управлением которой работают сервера – Scientific Linux (SL5). К важнейшим ресурсам комплекса относятся две системы хранения данных dCache, включающие 12 серверов – основных интерфейсов системы и 32 пула (системы хранения данных); а также три системы XROOTD, включающие сервер обработки запросов к системе и 12 пулов. Для обеспечения этих систем предоставляется около 1000 TB (1 PB) дискового пространства, организованного в RAID-массивы. Локальная сеть ЦИВК построена на базе агрегированных GigabitEthernet-соединений (транков), коммутаторов и маршрутизаторов HP Procurve и Cisco Catalyst.

Система была разработана на базе свободно распространяемого программного продукта Nagios, ряда дополнений к ней, а также написанных специально для нужд ЦИВК плагинов (подключаемых программных модулей) [Мирошникб 2003]. Модули Nagios являются исполняемыми файлами, возвращающими текстовое значение, реализуемы на любом удобном для этого языке (Perl, PHP, bash) и могут вызываться независимо от основного сервера, что упрощает их написание и отладку. Работа ядра Nagios заключается в запуске указанных для каждого свойства объекта (в терминах Nagios – сервиса) проверочных команд-сенсоров с заданными интервалами и, в случае возвращения командой статуса Warning либо Critical, оповещении указанных для сервиса контактов, а также обеспечении срабатывания при выполнении заданных условий обработчиков событий.

Основные классы задач мониторинга, решаемых разработанной системой:

1) мониторинг состояния вычислительных серверов: загрузка процессора, оперативной памяти, свободное пространство на жестком диске;

2) мониторинг дисковых массивов, используемых системами хранения данных;

3) мониторинг системы хранения данных dCache;

4) мониторинг сетевых устройств и агрегированных каналов (транков), генерация рекомендаций по балансировке трафика в соответствии с их состоянием;

5) мониторинг источников бесперебойного питания и вентиляционных блоков серверных стоек;

6) мониторинг доступности ряда общеупотребительных служб посредством запросов через соответствующие протоколы (SMTP, POP, DNS, E-mail, FTP, HTTP).

Для решения этих задач использовались как стандартные средства мониторинга тех или иных устройств и служб (например, утилиты arcconf, tw_cli для управления контроллерами RAID-массивов; запросы по протоколу SNMP для коммутаторов HP Procurve), так и более сложные алгоритмы и реализующие их программные средства, специально разработанные с ориентацией на повышение информативности системы. В таблице 1 представлены классы сообщений СЛМ ЦИВК ОИЯИ, выделенные на основе степени их информативности (приведены

Таблица 1. Классификация примеров диагностических сообщений, генерируемых системой локального мониторинга ЦИВК ОИЯИ, по степени информативности

<table>
<tr><td>1. Связанные с отсутствующим или неправильно настроенным компонентом системы мониторинга</td><td colspan="5">Связанные с реальной проблемой объекта мониторинга</td></tr>
<tr><td rowspan="3">CHECK_NRPE: Socket timeout after 30 seconds.<br>Connection refused by host<br>DISK UNKNOWN: Regular expression did not match any path or disk - /e/</td><td>2. Общая недоступность объекта</td><td colspan="4">Критическое состояние одного или нескольких параметров объекта</td></tr>
<tr><td rowspan="2">CRITICAL- Host Unreachable<br>PING CRITICAL - Packet loss = 100%</td><td>3. Общая неработоспособность некоторой локализованной составной части объекта</td><td colspan="3">Выход значения конкретного свойства объекта из допустимой области</td></tr>
<tr><td>1: DOWN (1 int NOK): CRITICAL - Port 01<br>No channels in Trunk (51)!</td><td>4. Сообщение содержит информацию только о факте несоответствия значения критерию</td><td>5. Сообщение содержит текущее значение параметра</td><td>6. Сообщение содержит дополнительную диагностическую информацию</td></tr>
<tr><td></td><td></td><td>CRITICAL - total memory is not 16438896 kB!<br>rdbl3 kernel: XFS: possible memory allocation deadlock in kmem_alloc (mode: 0x250)</td><td>CPU used 71.0% (>70) : WARNING<br>Output Current *125* Ampere 3~</td><td>RAID CRITICAL: Arrays OK but... 1 drive not OK - Status of drive in port p2 is DEGRADED (Array 0 on adapter 7)</td></tr>
</table>

примеры реальных сообщений для каждого класса). Справа налево возрастает величина *информативности* сообщений системы мониторинга, а с ней и практическая полезность сообщений. Подобная классификация сообщений позволяет рассмотреть дополнительный критерий качества СМ – среднюю информативность (*AvI*) ее сообщений за некоторый период времени. Для этого каждому сообщению присваивается некоторый *информационный вес* от 0 до 1 в соответствии с его положением в таблице. Так, сообщения класса 1 (левая колонка) могут иметь вес 0, т. к. эти сообщения вообще не несут информации, полезной для диагностики состояния подконтрольной системы и в ее рамках (но не в рамках объединенной системы) являются «информационным мусором». Сообщения класса 6, как предоставляющие максимально полную информацию, могут характеризоваться весом 1. После этого *AvI* рассчитывается по формуле

$$AvI = \frac{\sum_{i=1}^{k} I_{m_i}}{k}, \tag{2}$$

где $I_m$ – информационный вес сообщения $m$; $k$ – число сообщений, сгенерированных системой за расчетный период времени.

Для того чтобы учесть разницу в информационном весе различных сообщений и порождающих их сенсоров (методов), следует расширить область значения функции применимости $f_u$:

$$f_u = S \otimes P \to [0\ldots1],$$

причем

$$f_u(s, p) = AvI_{s,p},$$

то есть значение функции для некоторой пары свойства $p$ и сенсора $s$ определяется средней информативностью сообщений, порождаемых сенсором $s$ в процессе контроля над свойством $p$. Так, в случае неприменимости сенсора к контролю некоторого свойства все возможные сообщения, генерируемые им, будут принадлежать к классу 1, и, таким образом, значение функции применимости будет равно 0, как и в ее первоначальном виде.

Формулу (1) расчета меры определенности ТС подконтрольной системы нужно модифицировать, добавив для каждого контролируемого свойства множитель – коэффициент информативности (КИ), равный значению функции применимости для данного свойства и сенсора, применяемого для его контроля:

$$D = \frac{\sum_{i=1}^{c} f_{up_i} w_{p_i} n_{p_i}}{\sum_{j=1}^{d} w_{p_j} n_{p_j}}, \tag{3}$$

где $f_{up}$ и есть КИ, определяемый как значение функции применимости сенсора, отвечающего в системе за контроль свойства $p$.

Приведем таблицу, характеризующую рост меры определенности ТС ЦИВК ОИЯИ в ходе первого этапа развития системы локального мониторинга.

Таблица 2. Рост числа объектов мониторинга, типов сенсоров системы локального мониторинга и меры определенности технического состояния ЦИВК ОИЯИ

| **Дата оценки КИ и расчета D** | **17.08.2010** | **17.11.2010** | **10.02.2011** | **10.04.2011** | **10.08.2011** | **10.12.2011** |
|---|---|---|---|---|---|---|
| **Количество охваченных объектов ЦИВК** | 170 | 250 | 270 | 295 | 342 | 421 |
| **Количество типов сенсоров** | 24 | 26 | 26 | 30 | 36 | 41 |
| **Мера определенности D** | 0.6 | 0.74 | 0.76 | 0.8 | 0.87 | 0,93 |

В соответствии со спецификой контроля и обслуживания объекты локального мониторинга можно распределить по трем уровням: на нижнем, аппаратном, уровне осуществляется сбор и отображение данных об отдельных узлах сети, их аппаратном обеспечении и операционных системах; на сетевом уровне рассматривается состояние портов и каналов, устройств и служб, обеспечивающих работу локальной сети; на верхнем уровне – уровне служб – осуществляется контроль работы сервисов, предоставляемых конечным пользователям. Первоначально низкий уровень меры определенности обусловлен, во-первых, общей низкой информативностью сообщений стандартных плагинов Nagios, используемых в первой версии системы (по сути, определялись только доступность/недоступность объектов и нахождение параметров в заданных границах, без дополнительной информации о возможных причинах). Во-вторых, при выходе из строя объекта и, таким образом, выходе значений *всех* его свойств за установленные границы системой порождалось большое количество излишних сообщений о каждом из этих несоответствий. В-третьих, требовалось время для окончательного определения целесообразных пороговых значений всех свойств, многие из которых первоначально были выбраны недостаточно точно.

На практике повышение D достигалось за счет следующих мер в ходе развития системы мониторинга.

1. Обеспечение охвата каждого объекта сенсорами всех трех уровней, если это возможно. Для верной диагностики причин недоступности некоторого сервиса необходима информация о состоянии аппаратного обеспечения, поддерживающего его работу; для локализации или даже предупреждения проблем в системе хранения файлов, такой как dCache, необходимы данные, получаемые от контроллеров дисковых массивов, используемых этой системой.
2. Повышение числа распознаваемых состояний подконтрольного свойства для каждого сенсора системы и за счет этого повышение информативности сообщений, генерируемых этим сенсором – от простейшего «работает/не работает» к содержащим точную характеристику обнаруженной проблемы. Это не относится к сенсорам, предоставляющим точные числовые значения соответствующих свойств (температура, объем памяти и т. п.) – для них требовалось только постепенное уточнение границ допустимых значений.
3. Выявление и формализация зависимостей между объектами и их свойствами. Вообще, способность системы эффективно использовать информацию о подобных зависимостях между объектами и их свойствами (*Do*, *Dp*) в подконтрольной системе является одним из факторов, существенно влияющих на информативность СМ и, следовательно, определенность ТС подконтрольной системы.

Пусть между состояниями объектов $o_1$ и $o_2$ существует зависимость $do_{1,2}$ такая, что переход объекта $o_1$ в некоторое критическое состояние, характеризуемое сообщением $m_1$, вызывает переход $o_2$ в однозначно определяемое критическое состояние, характеризуемое сообщением $m_2$. Простейшими примерами таких объектов могут служить коммутатор некоторой подсети и принадлежащий к этой подсети компьютер – выход из строя первого приведет к сетевой недоступности второго. Аналогичный пример зависимости для свойств объектов $(Dp)$ – выход за установленные допустимые пределы времени выполнения тестового запроса к базе данных, с которой работает некоторый динамический веб-сайт (свойство $o_1s_1$, ситуация/сообщение $m_1$), приводит к увеличению времени отклика сайта $(o_2s_2, m_2)$, что, в свою очередь, вызывает снижение числа посещений страниц сайта $(o_2s_3, m_3)$.

В первом случае (коммутатор $o_1$ и компьютер $o_2$) сообщение $m_2$ (недоступность компьютера), несмотря на формальную принадлежность 2-й или даже 3-й категории по таблице 1, в реальности имеет нулевой коэффициент информативности, так как не дает никакой дополнительной (не содержащейся в $m_1$) информации о критической ситуации и бесполезно для ее локализации и устранения. Кроме того, недоступность компьютера $o_2$ будет означать переход в критическое состояние всех его свойств ($p_{o2}$ таких, что $f_c(p, o_2) = 1$), и сообщения $m_{po2}$, по-

рожденные этими состояниями, будут также иметь нулевой КИ, формально принадлежа к 1-й или 2-й категории по таблице 1. При этом возвращение $o_1$ в стабильное состояние автоматически приводит к возвращению в стабильное состояние всех $p_{o2}$.

Во втором случае способность СМ поддерживать зависимости между свойствами объектов и их свойств может привести к повышению коэффициента информативности сообщений $m_2$ и $m_3$. Полностью отказаться от генерации $m_2$ и $m_3$ нельзя, так как в отличие от первого примера $m_2$ и $m_3$ не обязательно имеют нулевой КИ (на переход $o_2s_2$ и $o_2s_3$ в критическое состояние могут влиять и другие факторы, помимо состояния $o_1s_1$).

Отметим, что приведенные формулы и определения можно расширить и для систем мониторинга, включающих все шесть подсистем, – тогда, помимо меры определенности ТС подконтрольной системы (критерия, ориентированного на подсистему оповещения), будет введен аналогичный критерий, ориентированный на подсистему коррекции. Если при формулировке рассмотренного выше критерия мы рассматривали сообщения, порождаемые подсистемой оповещения в ответ на нештатные состояния объектов мониторинга, то теперь вместо них нужно рассмотреть управляющие воздействия, порождаемые в тех же случаях подсистемой коррекции, и их эффективность. Формула для меры эффективности подсистемы коррекции, соответствующая формуле (3), будет выглядеть так:

$$E = \frac{\sum_{i=1}^{c} f_{ep_i} w_{p_i} n_{p_i}}{\sum_{j=1}^{d} w_{p_j} n_{p_j}}, \tag{4}$$

где $f_{ep_i}$ – оценка эффективности элемента подсистемы коррекции, осуществляющего управляющие воздействия над свойством $p_i$.

Применение рассмотренной методики дает возможность как оценить эффективность существующей или разрабатываемой системы мониторинга, так и выявить «узкие места», то есть ее неэффективно работающие элементы или участки подконтрольной системы, недостаточно охваченные сенсорами или средствами коррекции СМ.

## Список литературы

*Астахов Н. С., Долбилов А. Г., Иванов В. В., Кореньков В. В., Мицын В. В., Трофимов В. В.* Развитие Центрального информационно-вычислительного комплекса ОИЯИ в 2010–2011 году и текущее состояние программно-аппаратной среды // Научный отчет 2010–2011 Лаборатории информационных технологий, ISBN 978-5-9530-0312-4, 2012. – С. 16–20.

*Кореньков В. В., Дмитриенко П. В.* Архитектура и пути реализации системы локального мониторинга ресурсного центра // Электронный журнал «Системный анализ в науке и образовании», №3, 2011. – Дубна, 2011. URL: http://www.sanse.ru/download/96

*Мирошник И. В.* Теория автоматического управления. Линейные системы: Учебное пособие для вузов. – С.-Пб.: Питер, 2005. – 336 с.