УДК 004.738.52:004.031

А.И. Гриценко, В.И. Саенко

Харьковский национальный университет радиоэлектроники, Харьков

МЕТОД ВЫБОРА НАБЛЮДАЕМЫХ ПЕРЕМЕННЫХ ДЛЯ МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ

Рассматриваются вопросы сокращения избыточности передаваемых служебных данных в рамках развития теории и практики методологии мониторинга компьютерных сетей. Предложено развитие метода выбора наблюдаемых переменных для процессов мониторинга компьютерной сети. Все положения подтверждаются эксперементально, для получения экспериментальных данных используется технология мониторинга компьютерной сети WMI.

Ключевые слова: *компьютерная сеть, мониторинг, WMI, наблюдаемая переменная.*

Введение

Мониторинг компьютерной сети, как один из компонентов модели менеджмента OSI FCAPS [1], включает в себя функции контроля, анализа и визуализации состояния объектов компьютерной сети. Существующие на сегодняшний день программные системы мониторинга [2, 3] реализуют свои функции с помощью таких технологий как SNMP [4], WBEM, WMI [5], JMX [6]. Эти технологии основаны на архитектуре «агент-менеджер» и предоставляют стандартизированные механизмы централизованного сбора данных. При большом числе контролируемых объектов передаваемый поток информационных сообщений значительно снижает полезную пропускную способность компьютерной сети [7]. Для устранения этого явления эксперт или администратор компьютерной сети, реализующий мониторинг, должен соблюдать баланс между уровнем информационных затрат и степенью детализации объектов мониторинга. Как показывает практика, проблема снижения полезной пропускной способности компьютерной сети из-за процесса мониторинга нередко связана с избыточными информационными затратами, которые могут быть вызваны измерением не нужных для задач мониторинга переменных.

В общем случае снижение информационных затрат осуществляется различными техническими и организационными методами. Например, в [8] предлагается адаптивный метод снижения количества измерений. В [9] предлагается проводить измерения на удаленных объектах локально и передавать данные на сервер только при наступлении определенного события. Метод, предложенный в [10], основывается на идее пропуска плановых измерений и замене их интерполированными значениями. В [11] предлагается упорядочить всю организационную схему проведения мониторинга. Будем рассматривать только путь сокращения избыточности передаваемых данных.

Сокращение числа наблюдаемых переменных связано с проблемой выбора переменных из общего заранее определенного множества, доступного в рамках используемой технологии мониторинга. Как утверждается в [11], решение данной проблемы сложно представить в виде алгоритмической процедуры, так как выбор переменных основывается на опыте и интуиции эксперта, реализующего мониторинг. В данной работе предлагается вариант частичной формализации процедуры выбора наблюдаемых переменных.

Целью работы является разработка метода выбора наблюдаемых переменных для определенных условий задач мониторинга.

Структура статьи. В разделе 1 дано формализованное описание постановки задачи. В разделе 2 описаны концептуальные положения реализации мониторинга компьютерной сети и общая схема реализации мониторинга, дано описание решаемой задачи в виде математического выражения. В 3 разделе изложены результаты проведенной исследовательской работы: описана классификационная процедура наблюдаемых переменных, основывающаяся на специальных классификационных признаках. В 4 разделе пошагово представлен метод выбора наблюдаемых переменных для мониторинга компьютерной сети. В 5 разделе проводится оценка эффективности разработанного метода, используются специальные показатели уровня информационных затрат в процессе мониторинга и уровня детализации наблюдаемой системы. В 6 разделе приведен пример реализации предложенного метода на основе технологии WMI.

1. Постановка задачи

Предположим, что планируется проведение мониторинга состояния некоторой многосегментной компьютерной сети, при этом известна цель мониторинга G. Пусть для измерения переменных объектов мониторинга выбрана технология WMI,

предоставляющая сгруппированное множество переменных V, которые можно измерять и передавать по компьютерной сети.

Задача исследования сводится к разработке метода, реализующего некий функциональный оператор $\Phi(G,V)$, позволяющий выбрать сокращенный набор наблюдаемых переменных $\hat{V}$ из всего доступного множества V. При этом будем стремиться к минимизации потерь информативности описания наблюдаемого объекта и обеспечении исходной цели мониторинга G.

2. Концептуальные положения реализации мониторинга компьютерной сети

При инициализации процесса мониторинга задача эксперта или администратора сети заключается в выборе такого набора наблюдаемых переменных, который соответствовал бы поставленным целям мониторинга, формировал как можно более полную картину функциональности наблюдаемой системы и обеспечивал наименьшие информационные затраты в процессе передачи, обработки и хранения данных.

С формальной точки зрения – это оптимизационная задача. Но из-за слабой ее формализации, множества факторов, которые невозможно учесть, многокритериальности и динамичности, оптимальное решение получить невозможно и часто в этом нет необходимости. Многокритериальность приводит к противоречивым требованиям: с увеличением числа измеряемых переменных повышается степень детализации описания контролируемой системы, но снижается полезная пропускная способность компьютерной сети.

Для формального описания задачи выбора набора наблюдаемых переменных введем следующую терминологию:

– *показатель уровня информационных затрат* (I_c) – это количественный показатель, выражающий размер информационного потока, генерируемого в процессе измерения наблюдаемых переменных [бит\сек];

– *показатель степени детализации состояния наблюдаемой информационной системы* (I_d) – это количественный показатель, выражающий точность описания наблюдаемой системы, формируемой некоторым выбранным набором наблюдаемых переменных в определенном контексте решаемых задач мониторинга [%];

– *значимая наблюдаемая переменная* – это наблюдаемая переменная, которая удовлетворяет заранее оговоренным требованиям.

Введем также ограничения: I_c^* – максимально допустимое значение показателя I_c, I_d^* – максимально допустимое значение показателя I_d. Тогда задача выбора набора наблюдаемых переменных может быть представлена с помощью выражения

$$\begin{cases} \hat{V} = \Phi(G,V), \\ \hat{V} \subset V, \\ I_c^1 \le I_c^*, \\ I_d^1 \ge I_d^*; \end{cases} \quad (1)$$

где $\hat{V}$ – итоговое множество наблюдаемых переменных; Φ – функциональный оператор преобразования исходной цели мониторинга G и множества переменных V во множество $\hat{V}$; I_c^1, I_d^1 – показатели уровня информационных затрат и уровня детализации наблюдаемой информационной системы при измерении множества переменных $\hat{V}$.

Концепцию мониторинга будем рассматривать согласно обобщенной схеме, предложенной в [11]. Схема представляет собой пять этапов: *инициализация процесса измерений, планирование измерений, выбор инструментария для осуществления измерений, проведение измерений, обработка полученных данных*.

Первые три этапа реализации мониторинга являются подготовительными. Эксперт, реализующий мониторинг на этих этапах, должен обладать достаточным уровнем знаний о среде и объектах мониторинга, а также знать принципы и технологии мониторинга компьютерных сетей.

На этапе *инициализации процесса измерений* формулируется главная *цель мониторинга*. Четкая и лаконичная цель позволяет правильно определить решаемые *функциональные задачи*. Каждая задача требует определенного набора переменных.

На этапе *планирования измерений* определяются дополнительные критерии выбора переменных, выбирается частота измерений и архитектура системы менеджмента.

На этапе *выбора инструментария для осуществления измерений* выбирается технология мониторинга (SNMP [4], WMI [5], JMX [6]). На практике выбор технологии мониторинга может зависеть от множества факторов: конкретных объектов мониторинга, экономических ограничений, технической специализации экспертов, корпоративной политики и т.д. В рамках любой технологии мониторинга существует формальное описание всех переменных, которые могу быть измерены. Более того, все множество переменных разбито на *логические группы переменных*, сформированных по общим функциональным признакам. Это значительно упрощает эксперту задачу выбора *итогового множества переменных*.

Отправной точкой поиска *итогового множества переменных* является выбор *исходного множе-*

ства переменных, которое определяется экспертным путем на основании цели мониторинга. Например, если целью мониторинга является сбор статистики об использовании дискового пространства серверов, то в качестве *исходного множества переменных* будут рассматриваться переменные, характеризующие файлы, диски, файловую систему и соответствующее аппаратное обеспечение. Далее в рамках *исходного множества переменных* путем выбора логических групп, описанных в рамках используемой технологии мониторинга, формируется *начальное множество переменных*, которое на следующем шаге используется для формирования *итогового множества переменных* (рис. 1).

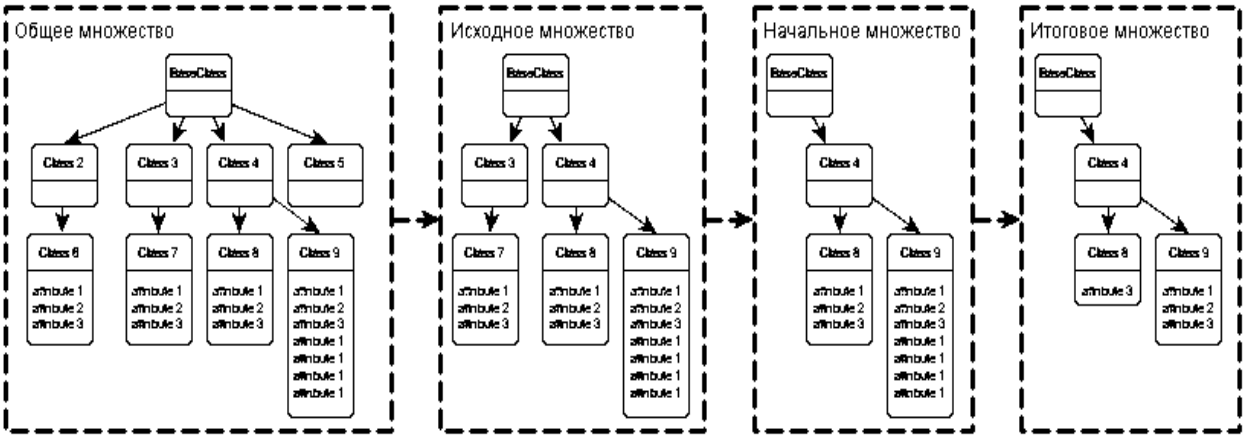

Рис. 1. Общая схема выбора наблюдаемых переменных

Общая схема реализации мониторинга [1] показывает, что чем больше измеряется переменных и чем выше частота измерений, тем больше требуется вычислительных, информационных и финансовых затрат.

3. Формирование решающих правил классификации

Методологическая основа предлагаемого решения для выбора наблюдаемых переменных основана на использовании специальных экспертных оценок о значимости той или иной переменной. Экспертные оценки предлагается использовать в специальных классификаторах. Основу классификаторов составляют классификационные признаки, которые характеризуют различные качества рассматриваемых переменных.

Особенность рассматриваемого подхода основана на некоторых предложениях. Для повышения гибкости процедуры оценивания (предоставления больше свободы для эксперта) предлагается ввести два пространства классификационных признаков: P_x и P_a.

Формирование классификационных пространств и классификационных признаков.

К пространству P_x принадлежат классификационные признаки, характеризующие в целом степень значимости наблюдаемых переменных для каждой из решаемых *функциональных задач*. Пространство P_a содержит *классификационные признаки*, которые более детально характеризуют степень значимости наблюдаемых переменных по их свойствам (статистическим, математическим и т.д.). Условно можно обозначить, что P_x содержит признаки состояния, а P_a – признаки поведения. Признаки обоих пространств формируются экспертным путем.

Для формирования множества классификационных признаков X пространства P_x на основании исходной цели мониторинга G определяются решаемые *функциональные задачи*. После чего каждой задаче ставится в соответствие один признак $x_i \in X$. Множество признаков A пространства P_a формируется путем выбора свойств наблюдаемых переменных, которые должны быть учтены во время экспертного оценивания. Выбор свойств осуществляется с учетом особенностей решаемых *функциональных задач*.

В результате, каждое выбранное свойство рассматривается как классификационный признак (классификационная переменная) $a_{ij} \in A$, расширяющий и дополняющий признак x_i.

Формирование классификационных уровней и областей.

Значения классификационных переменных будем определять в дискретной форме {1,0}. Наивысшая степень значимости наблюдаемой переменной выражается максимальным значением *классификационного признака* {1}. После экспертного оценивания значимости каждой переменной по соответствующему классификационному признаку предлагается рассчитывать обобщенную оценку. В качестве обобщенной оценки предлагается логическое

выражение

$$R = \bigvee_{i=1}^{n} (x_i \wedge (\bigwedge_{j=1}^{k_i} a_{ij})), \quad (2)$$

где x_i и a_{ij} равняется «0» или «1».

В выражении R связываются классификационные признаки пространств P_x и P_a, благодаря этому можно указать, какими свойствами должна обладать рассматриваемая переменная, при условии ее значимости для заданной функциональной задачи.

Формирование правила классификации.

Выбор переменных производим как процедуру классификации. В результате получим подмножество переменных с меньшей мощностью $M(\hat{V}) < M(V)$. Выбранные переменные будем называть *значимыми*. Они будут образовывать итоговое множество переменных мониторинга.

Основное правило классификации представляется в виде

$$\Re: v_i \in C_1 \mid R(v_i) = 1,\ i=1,..,m, \quad (3)$$

где C_1 – класс значимых переменных, m – мощность начального множества переменных.

Правило $\Re$ предполагает выполнимость условия, при котором рассматриваемая переменная принадлежит классу C_1 по определенным свойствам. В основе правила используется выражение (2), которое утверждает следующее: рассматриваемая переменная будет считаться *значимой*, если она значима по одному из признаков пространства P_x и по всем связанным с ним признакам пространства P_a.

Предложенная классификационная процедура состоит из двух этапов.

На первом этапе, на основании исходной цели мониторинга и признаков пространства P_x из *исходного множества переменных* формируется *начальное множество переменных* $\overline{V}$ путем выбора *групп переменных*.

На втором этапе с помощью признаков пространств P_x и P_a проводится экспертное и классификационное оценивание переменных *начального множества* $\overline{V}$ для получения *итогового множества переменных* $\hat{V}$.

4. Метод выбора наблюдаемых переменных для процесса мониторинга компьютерной сети

Предлагается метод, предназначенный для выбора наблюдаемых переменных для процесса мониторинга компьютерной сети.

Представим шаги метода:

1. Описывается цель мониторинга G и определяется исходное множество наблюдаемых переменных в рамках используемой технологии мониторинга.
2. Формируется множество классификационных признаков X пространства P_x. Формирование признаков обуславливается приоритетными функциональными задачами и реализуется экспертами.
3. На основании цели G и выбранных классификационных признаков X определяется начальное множество переменных $\overline{V}$ путем выбора априорных групп переменных.
4. Формируется множество классификационных признаков A пространства P_a. Формирование признаков реализуется экспертами с учетом особенностей решаемых функциональных задач и выбранных групп переменных.
5. Проводится экспертное оценивание всех переменных начального множества $\overline{V}$ с учетом их логической значимости. Для каждой переменной задаются значения классификационных признаков. Ставится «1», если переменная значима по заданному признаку, «0» в противном случае. Результаты оценивания записываются в таблицу.
6. Проводится классификационное оценивание всех переменных начального множества $\overline{V}$ путем вычисления выражения (2). Результаты записываются в таблицу.
7. С помощью правила классификации (3) проводится классификация переменных из множества $\overline{V}$ и формируется итоговое множество переменных $\hat{V}$.

5. Оценка эффективности разработанного метода

Оценить эффективность разработанного метода можно с помощью показателей уровня детализации состояния наблюдаемой информационной системы I_d и уровня информационных затрат I_c, рассчитываемых для процесса мониторинга. Считаем использование метода эффективным, если

$$I_c^1 \le I_c^*,\ I_d^1 \ge I_d^*, \quad (4)$$

где I_c^1, I_d^1 – показатели текущего уровня информационных затрат и уровня детализации наблюдаемой информационной системы при реализации мониторинга с помощью предложенного метода. В общем случае должно выполняться соотношение $I_c^1 < I_c^0$, $I_c^* < I_c^0$, $I_d^1 \approx I_d^0$, $I_d^* \approx I_d^0$, где I_d^*, I_c^* – пороговые допустимые значения показателей I_c^1 и I_d^1, I_d^0, I_c^0 – показатели I_d и I_c при измерении всех переменных общего множества. Оценивание I_d и I_c осуществляется в соответствии со специальными

методиками [9, 12, 14, 15].

6. Анализ полученных результатов

Основная идея и оригинальность предлагаемого метода состоит в следующем.

Во-первых, на начальном этапе, основываясь на экспертных оценках, предлагается из имеющегося множества переменных выбирать только ограниченное их число, формируя специальное множество переменных.

Во-вторых, выбор переменных осуществляется в соответствии со специальной процедурой классификации.

В-третьих, для формирования классификационных признаков предлагается выбирать набор основных показателей и показателей расширенных. Такой подход упрощает реализацию экспертного оценивания.

Три предлагаемых решения обусловливают новизну результата.

Недостаток предложенной методики – использование экспертных оценок, т.е. зависимость конечных результатов от квалификации эксперта. Но так как это разовая процедура и можно корректировать список переменных в текущем режиме, то недостаток можно не учитывать, контролируя условия (4).

7. Пример реализации метода

Рассмотрим на примере реализацию предложенного метода:

1. Пусть планируется решить задачу менеджмента производительности компьютерной сети. Для мониторинга выбрана архитектура «агент-менеджер», предполагающая централизованный сбор информации с рабочих станций. Согласно общей задаче цель задается как G – контроль производительности рабочих станций компьютерной сети. Для выбора контролируемых переменных будем полагать, что используется технология WMI [5], позволяющая измерять любые переменные в операционной системе, представленные информационной моделью CIM (общее множество переменных). Исходное множество переменных сформируем из переменных, характеризующих сетевое взаимодействие узлов компьютерной сети. В CIM эти переменные определены и описаны как «Formatted Performance Counters», они сгруппированы по 47 группам (наследники WMI класса Win32_PerfFormattedData [13]).

2. Согласно предложенному методу в соответствии с заданной целью зададим классификационные признаки пространства P_x. К таким признакам отнесем: контроль пропускной способности сети (x_1), контроль задержек, потерь и ошибок в процессе передачи данных (x_2) и контроль загруженности узлов базовыми сетевыми службами (x_3). Формирование признаков обусловлено приоритетными задачами и реализуется экспертами.

3. Определим начальное множество рассматриваемых переменных $\overline{V}$. Прежде всего, основываясь на выбранной цели и сформированных признаках X, выберем из 47 рассматриваемых групп переменных следующие группы: ICMP, IP, TCP, UDP. В WMI эти группы представлены классами

Win32_PerfFormattedData_Tcpip_ICMP,

Win32_PerfFormattedData_Tcpip_IPv4,

Win32_PerfFormattedData_Tcpip_TCPv4

Win32_PerfFormattedData_Tcpip_UDPv4.

Выбор групп обусловлен тем, что в рассматриваемой задаче используется только стек протокола TCP/IP v.4. Производительность будем оценивать как производительность передачи данных по протоколам TCP и UDP. Учитывая возможность появления «шумового» трафика и трафика специальных сообщений, дополнительно рассматриваем уровни IP и ICMP. Рассматриваемые группы состоят из следующего числа переменных: TCP – 9, UDP – 5, IP – 17, ICMP – 27 (всего 58 переменных).

4. Учитывая особенность рассматриваемых групп переменных и решаемых функциональных задач, сформируем классификационные признаки пространства P_a. Зададим требования, чтобы эти признаки учитывали особенность и режим измерения наблюдаемых переменных. Предлагаем следующий набор признаков: единицы измерения переменной – байт/с (a_{11}), переменная характеризует двунаправленный поток данных (a_{12}), переменная вариабельна (a_{13}, a_{21}, a_{31}), переменная характеризует локальную сторону сетевого взаимодействия (a_{22}, a_{32}), переменная измеряется при нормальном режиме функционирования сети (a_{23}, a_{33}).

5. Проведем экспертное оценивание значений всех переменных начального множества $\overline{V}$ с учетом их логической значимости. Ставим «1», если переменная значима по заданному признаку, «0» в противном случае. Результаты оценивания переменных группы IP приведены в табл. 1.

6. Проведем классификационное оценивание по каждой переменной, вычисляя выражение

$$R = (x_1 \wedge a_{11} \wedge a_{12} \wedge a_{13}) \vee (x_2 \wedge a_{21} \wedge a_{22} \wedge a_{23}) \vee (x_3 \wedge a_{31} \wedge a_{32} \wedge a_{33})$$

При этом

$$a_{13} = a_{21} = a_{31},\ a_{22} = a_{32},\ a_{23} = a_{33}.$$

Результаты оценивания переменных группы IP приведены в табл. 1.

7. В соответствии с предлагаемым методом

сформируем правило классификации $\Re$, проведем классификацию и сформулируем итоговое множество переменных

$$\Re: \ v_i \in C_1^{'} \mid R(v_i) = 1, \ i=1,..,58. \qquad (5)$$

В итоге по группе IP из 17 переменных выбираем 5. Рассматривая по аналогии группы TCP, UDP, ICMP, получаем из 58 переменных итоговое множество $\hat{V}$ из 18 переменных. Предложенная процедура не является оптимальной в смысле получения наилучших показателей «информативности» и «затрат».

Но учитывая, что удалось в 3 раза уменьшить число наблюдаемых переменных, показатель затрат $I_c^1 < I_c^*$. При этом считаем, что показатель информативности $I_d^1 \approx I_d^*$ незначительно уменьшился (риск эксперта).

Таблица 1

Результаты экспертного и классификационного оценивания наблюдаемых переменных группы IP

№ п/п	Переменная	x_1	x_2	x_3	a_{11}	a_{12}	a_{13} a_{21} a_{31}	a_{22} a_{32}	a_{23} a_{33}	R
1	Дейтаграмм/сек	1	0	0	0	1	1	0	1	**0**
2	Доставлено полученных дейтаграмм/сек	0	1	1	0	0	1	1	0	**0**
3	Исходящих дейтаграмм отброшено	0	0	1	0	0	1	1	1	**1**
4	Исходящих дейтаграмм с ошибкой 'Нет маршрута'	0	1	0	0	0	0	1	1	**0**
5	Полученных дейтаграмм отброшено	0	0	1	0	0	1	1	1	**1**
6	Отправлено дейтаграмм/сек	1	0	0	0	0	1	1	1	**0**
7	Ошибок при сборке фрагментов	0	1	0	0	0	1	0	1	**0**
8	Ошибок при фрагментации	0	1	0	0	0	1	1	1	**1**
9	Переслано дейтаграмм/сек	1	0	0	0	0	1	1	1	**0**
10	Получено дейтаграмм неопознанного протокола	0	1	0	0	0	0	0	1	**0**
11	Получено дейтаграмм с ошибками адреса	0	1	0	0	0	0	0	1	**0**
12	Получено дейтаграмм с ошибками заголовка	0	1	0	0	0	0	0	1	**0**
13	Получено дейтаграмм/сек	1	0	0	0	0	1	0	1	**0**
14	Получено фрагментов/сек	1	0	0	0	0	1	0	1	**0**
15	Собрано фрагментов/сек	0	1	1	0	0	1	1	1	**1**
16	Создано фрагментов/сек	0	1	1	0	0	1	1	1	**1**
17	Фрагментировано дейтаграмм/сек	0	1	1	0	0	1	1	0	**0**

Выводы

В результате решения поставленной задачи разработан метод выбора наблюдаемых переменных для процессов мониторинга компьютерной сети. Результаты получены путем экспертного анализа наборов переменных, которые стандартизированы и описаны в рамках технологии мониторинга WMI. Адекватность полученных результатов оценивалась путем реализации предложенного метода.

Сравнительный анализ предложенного метода показал его преимущества по сравнению с уже существующими методами, также ориентированными на снижение информационных затрат в процессе мониторинга компьютерной сети. Как упоминалось в разделе 1, решение проблемы снижения полезной пропускной способности компьютерной сети осуществляется различными техническими и организационными методами. По сравнению с методами, описанными в [8], [9], [10], предложенный в данной статье метод обладает рядом преимуществ: выбор переменных осуществляется до активной фазы мониторинга, что снижает риск негативного влияния избыточных информационных затрат, простая реализация благодаря простому математическому аппарату, возможность совместного использования со сравниваемыми методами без необходимости адаптации, отсутствие зависи-

мости от политик сбора данных. По сравнению с [11] предложенный метод предлагает более простую и лучше формализованную процедуру выбора наблюдаемых переменных.

Дальнейшее развитие метода предполагается направить по пути детального изучения свойств наблюдаемых переменных для повышения формализации выбора наблюдаемых переменных и получения в конечном итоге наилучших показателей уровня информационных затрат и уровня детализации наблюдаемой системы.

Научная новизна состоит в том, что получил дальнейшее развитие метод выбора наблюдаемых переменных для процесса непрерывного мониторинга компьютерной сети. Особенность метода заключается в предлагаемой формализованной процедуре выбора наблюдаемых переменных, которая основывается на процедуре классификации переменных с учетом их свойств, выраженных с помощью специальных классификационных признаков.

Практическая ценность заключается в реализации менее затратного процесса мониторинга, что эквивалентно снижению стоимости мониторинга.

Список литературы

1. *Clemm A. Network Management Fundamentals / A. Clem. Cisco Press. – 2006. – 510 с. – ISBN 1-58720-137-2.*
2. *List of systems management systems. [Электронный ресурс]. – Режим доступа к ресурсу: http://en.wikipedia.org/wiki/List_of_systems_management_systems.*
3. *Comparison of open source configuration management software. [Электронный ресурс]. – Режим доступа к ресурсу: http://en.wikipedia.org/wiki/ Comparison_of_open_source_configuration_management_software.*
4. *A Simple Network Management Protocol: RFC 1157. – [Действительный с 1990-05-01]. – SNMP Research. 1990. – 36 с.*
5. *Lavy M. Windows Management Instrumentation (WMI) / M. Lavy, A. Meggitt. – New Riders. – 2001. – 432 с. – ISBN 1-57870-260-7.*
6. *Java$_{TM}$ Management Extensions (JMX$_{TM}$): specification, version 1.4. [Действительный с 2006-11-09]. Sun Microsystems, 2006. – 290 с.*
7. *Bulut A. Optimization Techniques for Reactive Network Monitoring / A. Bulut, N. Koudas, A. Meka, A.K. Singh, D. Srivastava. – University of California, Santa Barbara. – 18 с.*
8. *Hernandez E. Adaptive Sampling for Network Management / E. Hernandez, M. Chidester, A. George // Journal of Network and Systems Management. – 2001. – Том 9, № 4. – С. 409-434.*
9. *Dilman M. Efficient Reactive Monitoring / M. Dilman, D. Raz // IEEE journal on selected areas in communications. – 2002. – Т. 20, № 4. – С. 668-676.*
10. *Саенко В.И. Метод выбора моментов измерений для процессов непрерывного мониторинга / В.И. Саенко, А.И. Грищенко // Радиоэлектроника и информатика. – 2007. – №4. – С. 119-122.*
11. *Hoeksema F.W. A Methodical Approach to Performance Measurement / F.W. Hoeksema, J.T. van der Veen, B.J. van Beijnum. – Enschede: Centre for Telematics and Information Technology. – 1997. – 113 с.*
12. *Yalagandula P. Correlations in End-to-End Network Metrics: Impact on Large Scale Network Monitoring / P. Yalagandula, S. Lee, P. Sharma, S. Banerjee. Phoenix: 11th IEEE Global Internet Symposium. – 2008. – 6 с.*
13. *Performance Counter Classes. [Электронный ресурс]. – Режим доступа к ресурсу: http://msdn.microsoft.com/en-us/library/aa392738(v=VS.85).aspx.*
14. *Jain A. Adaptive stream resource management using Kalman Filters / A. Jain, E. Y. Chang, Y.-F. Wang // SIGMOD. – 2004. – Вып. 4. – С. 11-22.*
15. *Babcock B. Distributed Top-K monitoring / B. Babcock, C. Olston // SIGMOD. – 2003. – Вып. 3. – С. 28-39.*

Поступила в редколлегию 1.02.2012

Рецензент: д-р техн. наук, проф. Н.И. Самойленко, Харьковская национальная академия городского хозяйства, Харьков.

МЕТОД ВИБОРУ СПОСТЕРЕЖУВАНИХ ЗМІННИХ ДЛЯ ПРОЦЕСІВ БЕЗПЕРЕРВНОГО МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

О.І. Гриценко, В.І. Саєнко

Розглядаються питання скорочення надмірності службових даних, що передаються, в рамках розвитку теорії та практики методології моніторингу комп'ютерних мереж. Запропоновано розвиток методу вибору спостережуваних змінних для процесів безперервного моніторингу комп'ютерної мережі. Усі положення підтверджуються прикладом. Експериментальні данні формуються за допомогою технології моніторингу комп'ютерної мережі WMI.

Ключові слова: *комп'ютерна мережа, моніторинг, WMI, спостережувана змінна.*

A METHOD OF CHOOSING OBSERVED VARIABLES FOR PROCESSES OF CONTINUOUS NETWORK MONITORING

O.I. Grytsenko, V.I. Saenko

This article presents a method of choosing observed variables for processes of continuous network monitoring. The suggested method is considered in the context of the developing the theory and practice of the information systems monitoring methodology. All statements are provided with an example. Experimental data are got within the network monitoring technology WMI.

Keywords: *computer network, monitoring, WMI, looked after variable.*