УДК 004.78

ПАРАМЕТРИЧЕСКИЙ СИНТЕЗ СИСТЕМЫ АКТИВНОГО МОНИТОРИНГА КОРПОРАТИВНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Надеждин Е.Н., Роганов А.А.

ФГБОУ ВО «Российский государственный гуманитарный университет», Москва, e-mail: en-hope@yandex.ru, andrej.a@mail.ru

Интенсивное развитие и внедрение сетевых технологий в сферу управления усложнило информационную инфраструктуру бизнес-систем и вызвало необходимость создания эффективных систем контроля и управления рисками информационной безопасности. В статье показана целесообразность включения в состав корпоративных вычислительных сетей специальных систем, осуществляющих удаленный мониторинг вычислительных ресурсов. Рассмотрены особенности активного мониторинга программных и аппаратных компонентов корпоративной вычислительной сети. Дана характеристика функционала и архитектуры типовой системы сетевого мониторинга. Перспективная система сетевого мониторинга должна обладать гибкой структурой и рядом интеллектуальных свойств, обеспечивающих накопление и интеллектуальный анализ данных, прогнозирование состояний защищенности и генерацию адекватного ответа при обнаружении аномалий. С учетом особенностей эксплуатации корпоративной вычислительной сети выделены основные показатели эффективности системы сетевого мониторинга. Предложена гипотеза расширения функциональности системы сетевого мониторинга на основе использования ресурсов прокси-сервера. Показана актуальность решения вопросов оптимального разграничения зон ответственности программных компонентов прокси-сервера. Задача распределения функций между компонентами программного обеспечения прокси-сервера сформулирована как специальная задача о назначении. Для численного решения комбинаторной задачи применён авторский алгоритм целочисленной оптимизации с использованием стандартной процедуры программного пакета MathCad 15. Представлены результаты поиска оптимального плана распределения сервисных функций на заданном наборе программных компонентов.

Ключевые слова: корпоративная вычислительная сеть, активный мониторинг вычислительных ресурсов, программное обеспечение, распределение функций между программными компонентами, задача о назначении, оптимальный план распределения

PARAMETRIC SYNTHESIS OF THE ACTIVE CORPORATE COMPUTER NETWORK MONITORING

Nadezhdin E.N., Roganov A.A.

Russian State University for the Humanities, Moscow, e-mail: en-hope@yandex.ru, andrej.a@mail.ru

The intensive development and implementation of network technologies in the management sphere has complicated the information infrastructure of business systems and necessitated the creation of effective control systems and information security risk management. The article shows the feasibility of including special systems for remote monitoring of computing resources into corporate computer networks. The features of active monitoring of software and hardware components of a corporate computer network are considered. The characteristics of the functionality and architecture of a typical network monitoring system are given. A promising network monitoring system should have a flexible structure and a number of intellectual properties that ensure data accumulation and intelligent analysis, prediction of security States, and generation of an adequate response when anomalies are detected. Taking into account the specifics of the operation of the corporate computer network, the main performance indicators of the network monitoring system are highlighted. The hypothesis of expanding the functionality of the network monitoring system based on the use of proxy server resources is proposed. The relevance of solving the issues of optimal delineation of the areas of responsibility of the software components of the proxy server is shown. The task of distributing functions between proxy server software components is formulated as a special assignment task. For the numerical solution of the combinatorial problem, the author's integer optimization algorithm was applied using the standard procedure of the MathCad 15 software package. The results of the search for the optimal distribution plan for service functions on a given set of software components are presented.

Keywords: corporate computer network, active monitoring of computing resources, software, distribution of functions between software components, assignment task, optimal distribution plan

Современный этап информатизации сферы управления бизнес-процессами характеризуется интенсивным развитием информационно-коммуникационной инфраструктуры промышленных предприятий и организаций различных форм собственности. Корпоративные информационно-вычислительные сети (КВС) сегодня рассматриваются как важнейший комплексный ресурс, необходимый для обеспечения конкурентоспособности организаций в условиях мирового экономического кризиса. В условиях непредсказуемости информационных угроз и деструктивных факторов различной природы на передний план сегодня вышла проблема комплексной защиты информационных ресурсов и активов предприятий и организаций. Перспективным направлением совершенствования защиты инфраструктуры и обеспечения устойчивости функционирования КВС является применение систем сетевого мониторинга,

на которые возлагаются ответственные задачи анализа состояния и контроля функциональности базовых компонентов аппаратного и программного обеспечения [1, 2]. Об актуальности вопросов совершенствования систем сетевого мониторинга (ССМ) убедительно свидетельствует возросший поток научных публикаций, посвящённых проблемам организации активного мониторинга и анализа данных, получаемых на его основе. Результаты мониторинга могут служить информационной базой для оперативной диагностики режимов работы коммутационного оборудования и узлов информационной сети вуза [3], для повышения эффективности распределенной библиотечной системы [4], для выявления потенциальных уязвимостей и оценки актуальных угроз в интересах управления рисками информационной безопасности [5, 6]. Общая тенденция в развитии ССМ заключается в интеллектуализации функционала, которая в значительной степени обусловлена интеграцией задач контроля и оперативного управления функциональным состоянием сетевых ресурсов [7]. В этой связи проблему создания систем активного функционального мониторинга ресурсов КВС необходимо рассматривать комплексно на основе методологии системного подхода с применением современных методов проектирования распределённых информационных систем [8].

Целью статьи является формализация и численное решение задачи оптимального распределения конечного набора заданных функций между программными компонентами прокси-севера, привлекаемого для осуществления регламента активного мониторинга программных и аппаратных средств (ПАС) КВС.

Традиционно мониторинг рассматривают как *специально организованное систематическое наблюдение за состоянием группы объектов, явлений и процессов в целях качественной и/или количественной оценки их состояния с априори заданных формальных позиций (аномальный характер поведения, работоспособность, надёжность, эффективность использования), а также протекающие при этом прикладные процессы (подпроцессы) в аспектах оценки состояния их качества и возможности использования в соответствии с принятым регламентом* [6]. При этом система мониторинга понимается как *комплекс специализированных программных средств, который должен позволять обслуживающему персоналу отслеживать функциональное состояние компонентов программного и аппаратного обеспечения КВС и своевременно реагировать на различные сбои и отклонения от штатного состояния*. Как показали наши исследования, автоматизация процедур администрирования при осуществлении активного мониторинга позволит существенно сократить объём информации, необходимой для эффективного управления рисками информационной безопасности (ИБ) КВС. Результаты мониторинга дают возможность не только документировать возникающие информационные инциденты, локальные проблемы и сбои, вызванные, например, перегрузкой сервера, отказом в доступе к сегментам базы данных, но в совокупности с учётными данными пользователей сети являются основанием для дополнительной аутентификации и обновления профилей активных пользователей сети. В свою очередь, анализ профилей пользователей системным администратором позволит своевременно выявить потенциального инсайдера и предотвратить несанкционированные действия и возможную утечку конфиденциальной информации.

По мнению ряда ведущих экспертов в области ИБ, активный функциональный мониторинг следует рассматривать как ключевой компонент сетевого администрирования и одновременно как информационный канал системы интегрированной защиты ресурсов инфраструктуры корпоративной КВС. На его основе могут быть построены гибкие автоматизированные механизмы контроля функционального состояния критических сегментов сети и аналитические схемы выявления и локализации потенциальных инсайдеров [5].

Анализ отечественного опыта разработки и эксплуатации КВС дает основание выделить основные требования к ССМ [9]: универсальность; масштабируемость; модульность структуры; защищенность; наличие простого и удобного интерфейса; наличие системы построения графиков и ведения истории; наличие системы оповещений; наличие системы визуализации данных. Перспективные ССМ должны, кроме того, предусматривать возможность включения нового оборудования и разработки новых плагинов для сбора данных с разнородных датчиков, интеграции с существующими техническими решениями и настройки расширений. К интеллектуальным функциям ССМ следует отнести возможность идентификации и сетевой интерпретации модели объекта мониторинга и настройку функционала ССМ под конкретную проблемную ситуацию.

Как показали наши ранние исследования [5, 6], для централизованного сбора и обработки информации о состоянии ре-

сурсов и действиях пользователей в КВС целесообразно установить специализированный сервер мониторинга. При выборе местоположения сервера следует руководствоваться рядом положений: минимальной удалённостью сервера от рабочих станций и ресурсов, мониторинг которых необходимо производить, защищённостью и достаточной ёмкостью линий связи между сервером мониторинга и рабочими станциями, которые будут к нему подключаться. Указанный сервер должен поддерживать активный мониторинг посредством генерации тестовых заданий и анализа логов аудита файловых систем и сетевого трафика. В частности, с прокси-сервера считывается лог сетевой активности пользователей, содержащий сведения о статистике их доступа к сетевым ресурсам. С контроллера домена может быть получена информация о неудачных попытках авторизации, о сессиях пользователей и т.п. Правомерно утверждать, что нагрузка на сервер мониторинга растет пропорционально объёму сетевого трафика и потока данных в контуре ССМ.

В статьях [9, 10] получила развитие идея создания кластерной системы сетевого мониторинга, позволяющей осуществлять оперативное наращивание дополнительных узлов системы при увеличении объема подключаемого оборудования многофункционального информационно-вычислительного комплекса. В нашей работе также примем гипотезу расширяющейся функциональности ССМ. При этом будем полагать, что дополнительные функции ССМ реализуются за счет привлечения свободных вычислительных и информационных ресурсов прокси-сервера. Указанное решение представляется обоснованным, учитывая уже реализованные функции прокси-сервера, связанные со сбором и предварительной обработкой данных о сетевом трафике. В состав программного обеспечения должны быть дополнительно включены программные компоненты, реализующие специальные функции обработки и интеллектуального анализа данных мониторинга состояния защищенности ПАС. В общем случае на прокси-сервер могут быть возложены следующие задачи:

– выявление подозрительной активности пользователей;

– обнаружение аномальных состояний трафика;

– цифровая фильтрация и предобработка первичных данных;

– поддержка процесса администрирования;

– накопление и визуализация статистических данных;

– сервисные функции.

В настоящей статье ограничимся рассмотрением вопросов, связанных с распределением ролей (функций) компонентов специального программного обеспечения (СПО) прокси-сервера, привлекаемого для информационной и вычислительной поддержки функционала расширяющейся системы активного мониторинга.

В интересах удобства формального представления рабочей модели примем условие, что СПО имеет модульную структуру. Для формализации задачи распределения набора заданных функций между программным компонентами СПО воспользуемся терминологическим аппаратом теории целочисленного программирования [11, с. 102–106].

Требуется найти оптимальный план распределения программных модулей (ПМ) $a_i \in A$, $i = \overline{1,m}$, СПО для выполнения заданной совокупности технологических операций (ТО) $u_j \in U$, $j = \overline{1,n}$. Пусть для осуществления каждой *j*-й операции может использоваться любой *i*-й программный модуль $a_i \in A$.

Введём булеву переменную $x_{i,j} = \{0, 1\}$, $i = \overline{1,m}$, $j = \overline{1,n}$

$$x_{i,j} = \begin{cases} 1, \text{ если } a_i \text{ включен в состав СПО и используется для выполнения операции } u_j; \\ 0, \text{ если } a_i \text{ не используется для выполнения операции } u_j. \end{cases}$$

Для оценки оптимальности плана введём функцию полезности модульного СПО

$$F(x) = \sum_{i=1}^{m} \sum_{j=1}^{n} (g_{i,j} \cdot h_{i,j} \cdot x_{i,j}). \qquad (1)$$

Здесь $0 < g_{i,j} \le 1$ – коэффициент матрицы полезности *G*, учитывающий влияние *j*-й операции в составе *i*-го программного модуля на качество мониторинга; $0 \le h_{i,j} \le 1$ – коэффициент матрицы предпочтительности, учитывающий предпочтительность выбора *i*-го ПМ для выполнения *j*-й операции с учетом условия нормировки $\sum_{j=1}^{n} h_{i,j} = 1 \ \forall i = \overline{1,m}$. Предположим, что для выполнения однотипных ТО в состав СПО включено несколько однотипных программных модулей. При этом каждый ПМ допу-

скает выполнение нескольких ТО. Данное условие отразим с помощью неравенства

$$1< \sum_{j=1}^{n} x_{i,j} \le r \quad \forall\, i = \overline{1,m}; \quad r = \text{const}. \qquad (2)$$

Затраты на компоненты СПО включают две составляющие:

а) приведенная стоимость, отражающая затраты на использование вычислительных ресурсов сервера

$$F_1(x) = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} \cdot x_{i,j} \le C_1, \qquad (3)$$

где $c_{i,j} \in C$ – стоимость ресурсов при реализации в ПМ a_i процедуры u_j;

б) приведенная стоимость, отражающая затраты на использование информационных ресурсов сервера

$$F_2(x) = \sum_{i=1}^{m} \sum_{j=1}^{n} s_{i,j} \cdot x_{i,j} \le C_2, \qquad (4)$$

где $s_{i,j} \in S$ – затраты ресурсов при реализации в ПМ a_i процедуры u_j.

Задача исследования состоит в определении бинарных значений управляемых переменных $x^* = (x_{i,j})$, $i = \overline{1,m}$, $j = \overline{1,n}$, при которых обеспечивается максимум функции полезности (1) и выполняются условия (2) и функциональные ограничения (3) и (4).

Сформулированная математическая модель оптимизационной задачи отличается от классической задачи о назначениях [11, с. 102], во-первых, снятием стандартного ограничения на число выполняемых функций через допущение $n > m$; во-вторых, введением функциональных ограничений (3) и (4); в-третьих, введением в качестве критерия оптимальности максимума дискретной функции полезности. Отметим также, что включение элементов матрицы $H = (h_{i,j})$ в структуру целевого функционала (1) позволяет гибко учитывать корреляцию технологических операций, совместно реализуемых в составе i-го программного модуля.

Исходные данные для решения контрольной задачи представлены в табл. 1–3.

Таблица 1

Затраты $c_{i,j} / s_{i,j}$ на использование вычислительных и информационных ресурсов сервера

$i \setminus j$	1	2	3	4	5	6	7	8
1	16/2	12/2	43/4	19/1	24/2	15/5	28/3	10/1
2	30/3	28/2	42/7	26/2	55/5	31/3	54/1	24/4
3	31/3	33/4	43/4	20/2	21/1	30/3	30/3	23/2
4	45/5	40/4	43/3	38/8	35/3	35/5	51/5	42/6
5	40/4	60/6	45/5	63/6	52/9	61/6	80/8	93/4

Таблица 2

Матрица коэффициентов полезности технологических операций $G = \{g_{i,j}\}$

$i \setminus j$	1	2	3	4	5	6	7	8
1	0.33	0.12	0.43	0.32	0.24	0.15	0.28	0.12
2	0.31	0.21	0.12	0.23	0.25	0.21	0.54	0.23
3	0.57	0.33	0.43	0.20	0.21	0.10	0.15	0.23
4	0.45	0.10	0.20	0.18	0.15	0.19	0.21	0.22
5	0.41	0.30	0.25	0.23	0.22	0.21	0.20	0.14

Таблица 3

Матрица коэффициентов предпочтительности $H = \{h_{i,j}\}$

$i \setminus j$	1	2	3	4	5	6	7	8
1	0.0	0.125	0.125	0.250	0.125	0.125	0.250	0.0
2	0.1	0.1	0.0	0.1	0.1	0.1	0.1	0.4
3	0.0	0.0	0.25	0.25	0.125	0.125	0.125	0.125
4	0.125	0.125	0.125	0.125	0.125	0.125	0.125	0.125
5	0.1	0.2	0.1	0.125	0.125	0.25	0.0	0.1

Сформулированная задача целочисленной оптимизации (1)–(4) в булевых переменных относится к классу NP-сложных комбинаторных задач. Поэтому для поиска оптимального плана распределения применён авторский алгоритм дискретной оптимизации, использующий унифицированную процедуру многопараметрической оптимизации, входящую в состав инструментальных средств математического программного пакета MathCad 15. При решении контрольной задачи использован опорный план управляемых переменных $x_0 = (x^0{}_{i,j}), i = \overline{1,m}, j = \overline{1,n}$:

$x_0 =$

0	0	0	1	0	0	0	1
1	0	0	0	1	0	0	0
0	1	0	0	0	0	1	0
1	0	1	0	0	0	0	0
1	0	0	0	0	1	0	0

Ниже приведён оптимальный план распределения $x^*{}_1 = \{x^*{}_{i,j}\}$, который определяет рекомендуемый вариант компоновки программных модулей.

$x_1^* =$

0	0	**1**	**1**	0	0	0	0
0	0	0	0	0	0	**1**	**1**
0	0	**1**	0	**1**	0	0	0
1	0	0	0	0	0	**1**	0
0	**1**	0	0	0	**1**	0	0

Достигнутые целевые показатели при использовании опорного плана $x_1 * = \{x^1{}_{i,j}\}$ представлены в табл. 4.

Таблица 4

Результаты решения задачи целочисленной оптимизации

$C_1 = 430,$ $C_2 = 40, r = 2$	Опорный план $x_0 = (x^0{}_{i,j}),$ $i = \overline{1,m}, j = \overline{1,n}$	Оптимальный план $x_1 * = \{x^1{}_{i,j}\}$
$F(x)$	0,329	0,632
$F_1(x)$	366	420
$F_2(x)$	35	38

Выводы

В статье сформулирована и решена задача выбора оптимального в смысле критерия максимума функции полезности плана распределения программных модулей прокси-сервера. Предложенная математическая модель специальной задачи о назначениях позволяет учитывать особенности архитектуры КВС и специфику ТО через назначение коэффициентов $\{g_{i,j}\}$ и $\{h_{i,j}\}$, а также вводить дополнительные функциональные ограничения и логические условия, связывающие управляемые переменные.

Реализация оптимального плана $x_1 * = \{x^1{}_{i,j}\}$ распределения программных модулей на множестве заданных функций предобработки данных, как показали расчеты, может сократить на 15–20 % затраты времени на сбор полной информации о функциональном состоянии ПАС и в целом повысить устойчивость работы ССМ в условиях расширения КВС. В контексте реализации требований политики корпоративной безопасности решение рассмотренной задачи будет способствовать созданию интеллектуальных механизмов защиты информации, адекватных характеру современных угроз в корпоративных КВС.

Список литературы

1. Сильнов Д.С. Актуальность удаленных систем современного мониторинга вычислительных ресурсов: состояние, проблемы, перспективы // Безопасность информационных технологий. 2011. № 3. Т. 18. С. 57–60.

2. Коноваленко С.А., Королев И.Д. Анализ систем мониторинга вычислительных сетей // Молодой ученый. 2016. № 23 (127). С. 66–73. [Электронный ресурс]. URL: https://moluch.ru/frchive/127/35280/ (дата обращения: 20.08.2020).

3. Рахман П.А. Средства мониторинга и диагностики информационно-вычислительной сети вуза // BC/NW 2006. № 2 (9):8.1. [Электронный ресурс]. URL: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=9&pa=8&ar=1 (дата обращения: 20.08.2020).

4. Усманов Р.Т., Кузнецов А.А. Служба мониторинга как средство повышения эффективности работы распределенной библиотечной сети АРБИКОН. Monitoring Service as a Means of Operation Efficiency Increase in the ARBIKON Distributed Library Network // Десятая юбилейная международная конференция и выставка «Libcom – 2006». Tenth jubilee international conference and exhibition: материалы конференции (г. Ершово, Московская обл., Россия, 13–17 ноября 2006 г.). Ершово, 2006. [Электронный ресурс]. URL: http://www.gpntb.ru/libcom6/disk/54.pdf (дата обращения: 20.08.2020).

5. Надеждин Е.Н., Цветков А.А., Шептуховский В.А. Оптимизация плана активного мониторинга ресурсов корпоративной вычислительной сети // Информатизация образования и науки. 2015. № 2 (26). С. 86–99.

6. Надеждин Е.Н., Цветков А.А. Синтез программы мониторинга ресурсов вычислительной сети образовательной организации // Интернет-журнал «Науковедение», 2014. № 5 (24). М.: Науковедение, 2014. [Электронный ресурс]. URL: http://naukovedenie.ru/PDF/36TVN514.pdf (дата обращения: 20.08.2020).

7. Васенин В.А., Жижченко А.Б. Алгоритмическое и программное обеспечение интернета следующего поколения // Информационное общество. Выпуск № 1. С. 56–64.

8. Лавров А.А., Лисс А.Р., Яновский В.В. Мониторинг и администрирование в корпоративных вычислительных сетях: монография. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2013. 160 с.

9. Кашунин И.А., Долбилов А.Г., Голунов А.О., Кореньков В.В., Мицын В.В., Стриж Т.А. Система мониторинга многофункционального информационно-вычислительного комплекса // CEUR Workshop Proc. (CEUR-WS.org). Aachen Univ.; RWTH. 2017. V. 1787. P. 256–263.

10. Кашунин И.А., Мицын В.В., Трофимов В.В., Долбилов А.Г. Интеграция кластерной системы мониторинга на базе Icinga2 в МИВК ЛИТ ОИЯИ // Письма в ЭЧАЯ. 2020. Т. 17. № 3 (228). С. 345–352.

11. Надеждин Е.Н., Смирнова Е.Е. Методы исследования операций: Основы теории и практики. Тула: Тульский государственный педагогический университет им. Л.Н. Толстого, 2018. 280 с.