УДК 004.056.5

Надеждин Евгений Николаевич
ФГАУ ГНИИ ИТТ «Информика»
Россия, Москва[1]
Главный научный сотрудник
Доктор технических наук, профессор
E-Mail: e.nadezhdin@informika.ru

Цветков Алексей Александрович
ФГБОУ ВПО «Ивановский государственный университет»
Шуйский филиал
Россия, Шуя[2]
Аспирант кафедры информационных систем и технологий
E-Mail: Tsvetkov.a.a@yandex.ru

Синтез программы мониторинга ресурсов вычислительной сети образовательной организации

Аннотация. Оперативное осуществление анализа данных о текущем состоянии сетевых ресурсов и несанкционированных действиях пользователей может служить информационной базой для выявления потенциальных уязвимостей, обнаружения инсайдеров компьютерной сети, настройки механизмов защиты ресурсов и снижения рисков информационной безопасности. В связи с чем актуальными являются проблемы организации активного мониторинга и интеллектуального анализа данных, получаемых на его основе. В данной работе сформулирована задача синтеза программы дистанционного мониторинга ресурсов распределенной вычислительной сети образовательной организации в интересах реализации автоматизированного ситуационного управления рисками информационной безопасности. При этом задача синтеза программы дистанционного мониторинга основана на оптимизации схемы обхода подконтрольных узлов сети для достижения наилучших значений показателей эффективности мониторинга ресурсов распределенной вычислительной сети. Постановка задачи синтеза преобразована к канонической модели задачи коммивояжера, для решения которой использован метод ветвей и границ. В настоящей статье также приведены результаты вычислительного эксперимента, в ходе которого определена оптимальная схема обхода узлов сети, приводящая к существенному снижению затрат времени и вычислительных ресурсов, что подтверждает эффективность применения разработанной методики.

Ключевые слова: распределённая вычислительная сеть; образовательная организация; дистанционный мониторинг ресурсов; активный мониторинг сети; задача синтеза программы мониторинга; оптимизация мониторинга; задача коммивояжера; метод ветвей и границ; обход узлов компьютерной сети; вычислительный эксперимент.

[1] 125009, Москва, Брюсов переулок, дом 21, строение 2
[2] 155908, Ивановская область, г. Шуя, ул. Кооперативная, д.24

Современный этап реформирования системы отечественного образования протекает на фоне интенсивного развития информационно-коммуникационной инфраструктуры образовательных организаций (ОО). Корпоративные информационно-вычислительные сети (ИВС) ОО сегодня рассматриваются как важнейший комплексный ресурс, необходимый для реализации ключевых положений новой образовательной парадигмы. В условиях вариативности трафика и непрерывного расширения спектра деструктивных факторов различной природы на передний план вышла проблема комплексной защиты ресурсов ИВС ОО [1, 4]. Перспективным направлением совершенствования защиты инфраструктуры и обеспечения устойчивости функционирования ИВС ОО является осуществление модели ситуационного управления ресурсами. В соответствии с современными взглядами, для реализации концепции ситуационного управления необходимо оперативно осуществлять анализ информации о текущем состоянии сетевых ресурсов и несанкционированных действиях пользователей. Об актуальности этих вопросов убедительно свидетельствует возросший поток научных публикаций, посвящённых проблемам организации активного мониторинга и интеллектуального анализа данных, получаемых на его основе. Такие сведения могут служить информационной базой для выявления потенциальных уязвимостей, обнаружения инсайдеров, настройки механизмов защиты ресурсов и снижения рисков информационной безопасности.

В настоящей статье рассматривается задача синтеза программы активного мониторинга ресурсов ИВС ОО в интересах реализации автоматизированного ситуационного управления рисками информационной безопасности. В качестве прототипа системы управления рисками выбрана концептуальная модель сетевой среды распределённых вычислений (ССРВ), изложенная в работе В.В. Корнеева [3]. В рамках известного подхода система управления ССРВ представляется в виде совокупности трех взаимодействующих подсистем:

1) подсистемы мониторинга, следящей за состоянием ресурсов и контролирующей состав ресурсов и режимы их функционирования;

2) подсистемы управления ресурсами, поддерживающей ресурсы в работоспособном состоянии, вводящей и выводящей их из процесса обработки и обеспечивающей их профилактику, ремонт и настройку;

3) подсистемы управления заданиями, динамично выделяющей ресурсы заданиям и управляющей заданиями в процессе их выполнения.

Уточним понятие мониторинга. *Мониторинг* будем рассматривать как *специально организованное систематическое наблюдение за состоянием группы объектов, явлений и процессов в целях качественной и/или количественной оценки их состояния с априорно 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* [7]. В качестве прототипа рабочей модели мониторинга ресурсов распределённой ИВС ОО, используемой в наших исследованиях, выбрана известная подсистема мониторинга ресурсов среды распределённых вычислений, построенная на базе информационной службы MDS, свободно распространяемого продукта Globus Toolkit, протокола LDAP и механизма активного мониторинга FLAME [1]. Под термином «*мониторинг состояния защищенности ресурсов*» далее понимается совокупность подпроцессов, которые предусматривают систематическое дистанционное зондирование и наблюдение за функциональным состоянием и защищенностью ресурсов ИВС с целью обнаружения имеющихся или возникающих в результате несанкционированных действий пользователей уязвимостей [2, 7].

Мониторинг сегментов ИВС обычно сводится к целенаправленному автоматизированному или автоматическому прямому (или косвенному) дистанционному наблюдению за действиями пользователей в интересах своевременного обнаружения попытки или факта нарушений установленных прав доступа и обеспечивая сбора информации о «подозрительном» поведении пользователей на критическом сегменте сети [7]. Выделим основные функции системы мониторинга ресурсов ИВС в контуре управления рисками информационной безопасности:

а) слежение за состоянием информационных и вычислительных ресурсов;

б) оценка достаточности имеющихся ресурсов;

в) контроль их определяющих характеристик и режимов функционирования;

г) оценка активности пользователей на заданном сегменте ИВС ОО.

Конфигурированию системы мониторинга должны предшествовать анализ характеристик архитектуры ИВС, прогнозирование характера и направленности вероятных угроз и определение оптимального плана размещения инструментов мониторинга. В последнее время все более распространенной стала «клиент-серверная» модель взаимодействия компьютеров в ИВС, состоящая из нескольких неравноправных звеньев: серверов, владеющих информационными ресурсами, и клиентов, имеющих возможность обращаться к этим ресурсам. В этой связи сетевая модель активного мониторинга рабочих станций ИВС на содержательном уровне может быть представлена в следующем виде. Все компьютеры ИВС ОО объединены в домен. В ИВС могут быть размещены различные сервера: прокси-сервер, файловый сервер, сервер баз данных, сервер Backup, контроллер домена, сервер администрирования антивирусов и другие. В ИВС присутствуют рабочие станции пользователей, каждая из которых имеет свою доменную учетную запись, определяющую права доступа к корпоративным сетевым и к интернет-ресурсам.

Как показали наши исследования [7, 9], для централизованного сбора и обработки информации о состоянии ресурсов и действиях пользователей в ИВС целесообразно установить специализированный сервер мониторинга. При выборе местоположения сервера необходимо руководствоваться несколькими критериями: минимальной удалённостью сервера от рабочих станций (РС) и ресурсов, мониторинг которых необходимо производить, защищённостью и достаточной ёмкостью линий связи между сервером мониторинга и РС с клиентами, которые будут к нему подключаться. Указанный сервер должен поддерживать активный мониторинг посредством генерации тестовых заданий и анализа логов аудита файловых систем и сетевого трафика. Так, например, с прокси-сервера считывается лог сетевой активности пользователей, содержащий в себе сведения об успешных и неудачных попытках их доступа к сетевым ресурсам. С контроллера домена может быть получена информация о неудачных попытках авторизации, о сессиях пользователей и т. п.

Выбор конкретных средств и методов сетевого мониторинга должен опираться на такие факторы, как конфигурация сети, наличие действующих серверов, характеристики установленного программного обеспечения и другие. Однако в любом случае представляется целесообразным активизация и сопровождение двух параллельных информационных процессов – общего и событийного видов мониторинга. *Общий мониторинг* должен проводиться с некоторой периодичностью, определяемой политикой безопасности ОО и параметрами ИВС, и состоять из следующих последовательных действий: тестирование физической доступности оборудования; анализ работоспособности критических служб и сервисов, запущенных в сети; проверка функционального состояния всех компьютеров в ИВС и состояния баз данных. *Событийный мониторинг* проводится при появлении определенных критических событий, возникающих как при работе пользователей, так и сетевого

оборудования и внешних систем. При этом регистрируется само событие и все связанные с ним изменения данных. Отчеты по результатам общего и событийного видов мониторинга систематизируются и отправляются в установленном формате в базу данных мониторинга.

Система мониторинга должна быть спроектирована, ориентируясь на конкретные задачи и технологические возможности управления ресурсами распределённой ИВС ОО. При этом функционирование такой системы должно осуществляться в режиме регламентного времени, не нарушая режим работы ИВС, при возможном минимуме привлекаемых информационных и вычислительных ресурсов. Для оценки эффективности программы мониторинга необходимо определить количественные характеристики мониторинга применительно к определённым условиям его проведения. Ключевыми показателями эффективности мониторинга могут служить: качество собранной информации, затраты времени на проведение мониторинга и его периодичность, ресурсозатратность [3, 8]. В интересах формализации задачи синтеза программы активного мониторинга, ограничимся рассмотрением трёх основных показателей:

1) длительность полного цикла T_{Σ} мониторинга ресурсов выделенного сегмента ИВС;
2) приведённая величина затрат N_{Σ}^{Π} вычислительных ресурсов, определяемых количеством вычислительных операций;
3) достоверность гипотезы о работоспособном состоянии ресурсов, необходимых для выполнения $k-й$ функциональной задачи, в виде условной вероятности P_y^k на основании обработки результатов мониторинга.

Добиться наилучших значений показателей можно путём оптимизации схемы обхода подконтрольных узлов сети, под которой будем понимать такой способ его осуществления, при котором временные затраты являются минимальными, а затраты вычислительных ресурсов и достоверность мониторинга находятся в допустимых пределах. Учитывая специфику топологии распределённой ИВС ОО, предлагается процесс мониторинга ресурсов осуществлять в несколько этапов:

1) идентификация рабочей сетевой модели ИВС;
2) сегментация сетевой модели ИВС;
3) оптимизация программы мониторинга и выбор механизмов её реализации;
4) собственно осуществление мониторинга;
5) обработка и анализ результатов мониторинга.

В настоящей статье ограничимся рассмотрением второго и третьего этапов активного мониторинга.

Предположим, что рабочая модель распределённой ИВС ОО с известной архитектурой представлена функциональным графом $G(X,U)$, где X - множество вершин, U - множество дуг. Пусть *задача сегментации* заключается в декомпозиции рабочей модели $G(X,U)$ и в выделении совокупности относительно независимых подсистем (сегментов), связи между которыми могут быть условно разомкнуты (с последующим учётом) без ущерба для результата исследования. Произвести декомпозицию сложной системы управления - это значит выделить в ней отдельные сильно связанные подсистемы, т. е. такие подсистемы, все остальные части которых благодаря обратным связям взаимно достижимы. Известно, что граф такой системы бисвязен. При декомпозиции ИВС выделяются также слабо связанные

подсистемы, все составные части которых связаны неориентированным путем. Граф такой подсистемы связен. Предложим формализацию решения задачи декомпозиции ИВС на основе сокращения размерности ориентированного функционального графа $G(X,U)$. Для упрощения модели распределённой инфраструктуры ИВС, представленной ориентированным графом, можно рекомендовать следующий алгоритм декомпозиции [6].

ШАГ 1. Составить матрицу смежности A графа $G(X,U)$.

ШАГ 2. Сформировать вспомогательную матрицу $R_1 = A + E$, где E - единичная матрица размера $(n \times n)$; (+) – знак логического сложения; R_1 – матрица первой достижимости, i-я строка которой представляет все ориентированные пути по графу из i-й вершины до всех остальных вершин, если длина пути равна одному ребру.

ШАГ 3. Определить $R_2 = R_1^{*2}$, где символ $(*)$ означает, что при вычислении $R_1 \times R_2$ применяется логическое умножение и суммирование соответствующих элементов матриц.

Аналогично определяются все матрицы вплоть до $R = R_n = R_1^{*n}$, где R – матрица достижимости графа $G(X,U)$, i-я строка которой представляет все ориентированные пути по графу длиной от одного до n ребер из i-й вершины ко всем остальным. Матрицы A и R имеют размерность $n \times n$.

При вычислении R не обязательно R_1 возводить в n-ю степень. Если $R_1^{*k} = R_1^{*(k-1)}$, то $R = R_1^{*k}$, где $k < n$.

ШАГ 4. Проанализировать матрицу R. Здесь возможны два случая. Если $R = Q$, где $Q = [q_{ij}]$ - такая универсальная матрица, что для всех индексов i и j выполняется условие $q_{ij} = 1$, то граф бисвязен, и декомпозиция системы невозможна. При этом система состоит из одной сильно связанной подсистемы. Если $R \neq Q$, то необходимо перейти к следующему шагу. В тех случаях, когда априорно известно, что граф связен, следует перейти к шагу 8.

ШАГ 5. Определить матрицу достижимости неориентированного графа $G^0(X,U)$, соответствующего ориентированному графу $G(X,U)$ системы. Матрица $R^0 = (A + A^T + D)^{*n}$, где символ «Т» означает операцию транспонирования.

ШАГ 6. Определить связные подграфы ориентированного графа $G(X,U)$. Известно, что множество вершин связного подграфа, содержащего вершину i, определено единицами в i-й строке матрицы R^0. Если $R^0 = Q$, то граф $G(X,U)$ состоит из одного связного подграфа. В этом случае необходимо перейти к шагу 8. Если же $R^0 \neq Q$, то надо перейти к следующему шагу.

ШАГ 7. Упорядочить вершины графа $G(X,U)$ (матрицы A) по связным подграфам.

ШАГ 8. Образовать матрицу связности $C = R + R^T$. Здесь предусмотрена обычная (арифметическая) операция сложения.

ШАГ 9. Выделить из матрицы C бисвязные подграфы. Бисвязный подграф, содержащий вершину k, определен двойками в k-й строке матрицы C.

ШАГ 10. Упорядочить матрицу A так, чтобы бисвязные подграфы образовали квадратные подматрицы $E_\mu \subset A,\ \mu = \overline{1, p}$.

ШАГ 11. Образовать матрицу $R_+ = (A_+^0 + A_+^T + E_+)^{*\mu}$, где A_+ - матрица смежности подграфа с множеством вершин $H = W / \overset{w}{\underset{\mu=1}{U}} B_\mu$, B_μ – подмножество составных частей μ-й сильно связанной подсистемы, а затем выполнить п. 6 и п. 7.

ШАГ 12. По упорядоченной матрице A' определить связи (ребра) между подсистемами, которые могут быть разорваны в результате декомпозиции.

Рассмотрим пример реализации изложенного алгоритма декомпозиции. Пусть известна ИВС, структура которой представлена графом, приведённым на рис.1 (разработан авторами). Составим матрицу смежности A этого графа. Далее последовательно получим матрицу достижимости R этого графа и матрицу связности C.

Изучая структуру матрицы R_+^0, выделяем дополнительно три слабо связанные подсистемы B_3 ={1, 4, 5}, B_4 ={12, 14} и B_5 ={2}.

Анализируя структуру матрицы связности C, выявляют две сильно связанные подсистемы B_1=(6, 7, 8, 9, 10) и B_2 = (3, 11, 13, 15, 16).

***R*=**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1															2
	1	1								1		1		1	1	3
	1	1	1		1	1	1	1	1	1	1	1	1	1	1	4
	1	1		1	1	1	1	1	1	1	1	1	1	1	1	5
	1	1			1	1	1	1	1	1	1	1	1	1	1	6
	1	1			1	1	1	1	1	1	1	1	1	1	1	7
	1	1			1	1	1	1	1	1	1	1	1	1	1	8
	1	1			1	1	1	1	1	1	1	1	1	1	1	9
	1	1			1	1	1	1	1	1	1	1	1	1	1	10
	1	1								1		1		1	1	11
	1	1								1	1	1	1	1	1	12
	1	1								1		1		1	1	13
	1	1								1		1	1	1	1	14
	1	1								1		1		1	1	15
	1	1								1		1		1	1	16

C=

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
2																1
	2															2
		2								2		2		2	2	3
			2													4
				2												5
					2	2	2	2	2							6
					2	2	2	2	2							7
					2	2	2	2	2							8
					2	2	2	2	2							9
					2	2	2	2	2							10
		2								2		2		2	2	11
											2					12
		2								2		2		2	2	13
													2			14
		2								2		2		2	2	15
		2								2		2		2	2	16

Из полученных результатов следует, что в упорядоченной матрице смежности A' функционального графа $G(X,U)$ необходимо разорвать связи, выделенные на матрице звездочкой, а на рис. 1 крестиками. После декомпозиции матрицу A' можно разрушить, сохранив лишь подматрицы смежности D_s и матрицу смежности сокращенного графа M, которые естественным образом получаются из A'.

A' =

1	4	5	6	7	8	9	10	12	14	3	11	13	15	16	2	
	1	1														1
			1*													4
						1*										5
				1												6
					1											7
						1		1*								8
							1									9
			1													10
									1							12
													1*		1	14
												1				3
										1			1	1		11
											1				1*	13
																15
												1				16
																2
***B*3**			***B*1**					***B*4**		***B*2**					***B*5**	

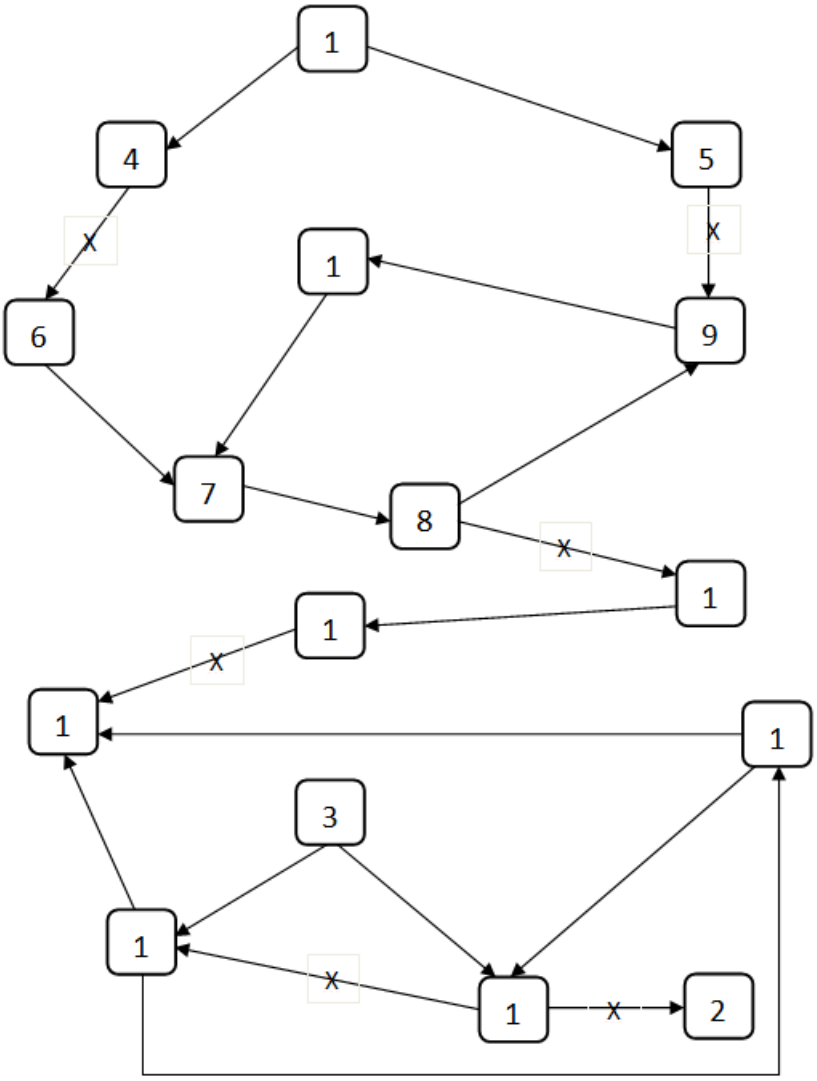

Рис. 1. *Исходный функциональный граф ИВС ОО*

Замкнутые контуры в подсистемах B_1 и B_2 устраняются на основе использования матриц смежности.

D_1=

6	7	8	9	10	
	1				6
		1			7
			1		8
				1	9
1					10

D_2=

3	*11*	*13*	*15*	*16*	
		1			*3*
1			1	1	*11*
	1				*13*
				1	*15*
		1			*16*

После декомпозиции и устранения замкнутых контуров можно представить ИВС сокращенным ориентированным графом $Z(V,E)$, где V – множество вершин (подсистем); E – множество ориентированных ребер (связей между подсистемами).

Полученный сокращенный граф является удобной моделью для решения динамических, информационных и диагностических задач при проектировании ИВС ОО. Он обладает всеми основными топологическими свойствами исходной модели ИВС, поскольку система преобразовывалась таким образом, чтобы топологическое пространство, представленное ориентированным графом G(X,U), непрерывно отображалось в топологическое пространство, представленное графом $Z(V,E)$. Для рассмотренного примера матрица смежности M сокращенного графа $Z(V,E)$ (рис. 2, разработан авторами) имеет вид:

M=

B_1	B_2	B_3	B_4	B_5	
			1		B_1
				1	B_2
1					B_2
	1				B_2
					B_2

Во всех матрицах рассмотренного примера, за исключением случая матрицы C, в свободных клетках подразумеваются нули; а в матрице C все свободные клетки заполнены единицами.

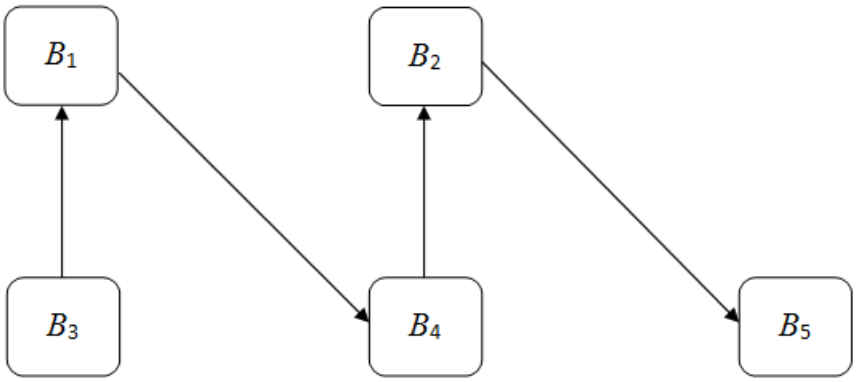

Рис. 2. *Укрупненная функциональная модель ИВС ОО после сегментации*

Полученная на втором этапе исследования графическая модель (рис. 2) с общих позиций описывает взаимодействие компонентов ИВС.

Поставим в соответствие каждому сегменту B_k, $k=\overline{1,m}$, вершину W_k, $k=\overline{1,m}$. Дополнительно введём вершину W_{m+1}, которая будет имитировать использование сервера мониторинга ресурсов ИВС. Множество вершин W_k, $k=\overline{1,(m+1)}$ соединим множеством дуг единичных (i,j), которые будут отражать информационные связи между соответствующими вершинами. Полученный ориентированный граф $Z^*(W,E)$ модели представлен на рис. 3 (разработан авторами).

Положим, что $m+1=n$.

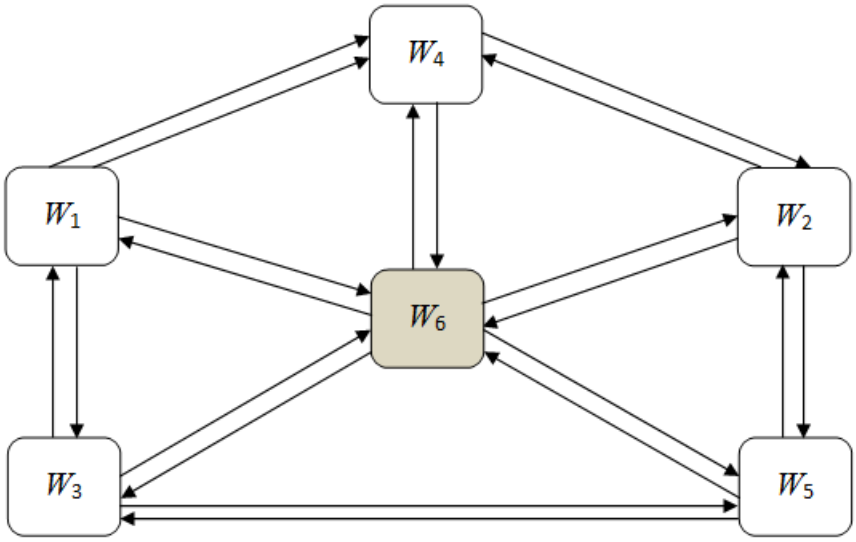

Рис. 3. *Модифицированный граф рабочей сетевой модели*

В целях упрощения графического представления модели на рис.3 покажем только дуги (i, j), которые связывают дополнительную вершину W_n с остальными вершинами W_k, $k = \overline{1,m}$. Веса всех дуг зададим с помощью квадратной матрицы $C(i, j) = [c_{i,j}]$ размерности $n \times n$, полагая при этом, что $c_{i,i} = \infty \ \ \forall\, i = \overline{1,n}$.

Учитывая принятые допущения, исходная задача синтеза программы мониторинга ресурсов ИВС ОО может быть интерпретирована как комбинаторная задача поиска оптимального в смысле суммарных затрат замкнутого маршрута L^*. Такой маршрут должен начинаться в вершине W_n и проходить один раз через все остальные вершины W_k, $k = \overline{1,m}$, модифицированного графа рабочей модели (рис. 3). Конкретизируем физический смысл элементов $c_{i,j}$, $i, j = \overline{1,n}$. Предварительно отметим, что автоматизированная обработка информации о функциональном состоянии очередного j-го сегмента сети предполагает использование априорной информации. Одним из источников такой информации могут быть результаты анализа состояния i-го сегмента, осуществлённого на предыдущем шаге мониторинга.

Пусть элемент $c_{i,j}$ отражает полные затраты времени на функциональную диагностику j-го сегмента после полной проверки i-го сегмента сети: $T_j(i) = t_1^i + t_2^i + t_3 + t_4^i + t_5$, где t_1^i – среднее время актуализации инструментов мониторинга при переходе к новому сегменту ИВС ОО; t_2^i – время, требуемое для сбора, анализа и систематизации априорных данных; t_3 – время, требуемое для генерации тестовых заданий; t_4^i – время, необходимое для проверки функциональности сегмента; t_5 – время обработки результатов тестирования и идентификации функционального состояния сегмента. Значения составляющих t_1^i, t_2^i и t_3^i существенно зависят от предыстории мониторинга, т.е. от особенностей тестирования предшествующего i-го сегмента. В случае линейной аппроксимации можно полагать, что время $T_j(i)$ эквивалентно некоторому обобщённому «расстоянию» между смежными сегментами и может быть представлено в виде: $T_j(i) = c_{i,j} \cdot \Delta\tau$. Здесь $\Delta\tau$ – априорно заданный

квант времени, а $c_{i,j}$ – полные затраты времени на осуществление мониторинга j-го сегмента, выраженные в числе квантов времени. Предложенный подход позволяет рассматривать исходные данные в относительных условных единицах (у.е.), что существенно упрощает их обоснование и использование. Аналогично рассуждая, можно ввести относительные показатели и для оценки вычислительных затрат при реализации процедур мониторинга.

Используя введённые обозначения, задача синтеза программы мониторинга может быть сведена к решению известной задачи коммивояжера [2]. Рассмотрим формальную модель канонической задачи коммивояжера.

Задано n пунктов, пронумерованных числами $1, 2, 3,..., n$. Для любой пары пунктов (i, j) задано обобщённое расстояние $C(i, j) = c_{i,j} > 0$ между ними, которое учитывает затраты времени и расход ресурсов. В общем случае принимается, что $C(i, j) \neq C(j, i)$. Коммивояжер, выезжая из какого-либо пункта, должен посетить все пункты по одному разу и вернуться в исходный пункт. *Требуется определить* такую последовательность обхода пунктов, при которой общая длина маршрута перемещения (полные затраты ресурсов) коммивояжера была бы *минимальной.*

Рассмотрим постановку задачи в терминах теории целочисленного линейного программирования [1]. Введём вспомогательные булевы переменные $x_{ij} = \{0; 1\}, i, j = \overline{1, n}$, следующим образом: $x_{ij} = 1$, если коммивояжер переезжает из i-го пункта в j-й пункт; $x_{ij} = 0$ – в противном случае. Тогда задача заключается в определении значений переменных x_{ij}, удовлетворяющих следующим соотношениям:

$$F(x) = \sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij} \cdot x_{ij} \to \min . \quad (1)$$

при условиях $\sum_{i=1}^{n} x_{ij} = 1$, $j = 1,..., n$ (въезд в пункт j); (2)

$$\sum_{j=1}^{n} x_{ij} = 1, \; i = 1,..., n \text{ (выезд из пункта } i). \quad (3)$$

$$u_i - u_j + n \cdot x_{ij} \leq n - 1 , (i \neq j); \quad (4)$$

$x_{ij} = \{0; 1\}$, $u_i \geq 0$ - произвольные вещественные числа, $i, j = 1,..., n$. (5)

Ограничения (4) означают, что маршрут коммивояжера должен образовывать контур.

Задача коммивояжера, как известно, относится к классу NP-сложных задач дискретной оптимизации, для которых не существует единого универсального алгоритма решения. Рассмотрим решение задачи коммивояжера на основе метода ветвей и границ [2]. Допустимый маршрут x с учётом принятых обозначений представим как множество упорядоченных пар пунктов $x = \{(i_1, i_2), (i_2, i_3),..., (i_{n-1}, i_n), (i_n, i_{n-1})\}$.

Каждый допустимый маршрут будем рассматривать как цикл, проходя по которому коммивояжер посещает каждый пункт ровно один раз и возвращается в исходный пункт.

Каждая упорядоченная пара (i, j) образует элементарную коммуникацию и является дугой маршрута. Длина $F(x)$ маршрута x равна сумме соответствующих элементов $C(i, j)$. Заметим, что множество всех допустимых маршрутов $X = (x_1, x_2, ..., x_p)^T$ содержит $(n-1)!$ элементов.

Обозначим матрицу расстояний через $C = (c_{i,j})_{nxn}$. Чтобы исключить переезды типа (i,i), введём условие $C(i,i) = +\infty \; \forall \; i = 1,...,n.$ Пусть $P_i = \min\{c_{i,j}\}, \; j = 1,...,n,$ $Q_j = \min\{c_{i,j} - P_i\}, \;\; i = 1,...,n,$ $\overline{C_{i,j}} = c_{i,j} - P_i - Q_j$. Тогда $\overline{C} = (\overline{C}_{i,j})_{nxn}$ - редуцированная матрица.

Пусть $d(X) = \sum_{i=1}^{n} P_i + \sum_{j=1}^{n} Q_j$ - сумма констант редуцирования. Тогда для любого маршрута $x = \{(i_1, i_2), (i_2, i_3), ..., (i_{n-1}, i_n), (i_n, i_{n-1})\} \in X$ имеем

$$F(x) = C(i_1, i_2) + C(i_2, i_3) + ... + C(i_n, i_1) = \overline{C}(i_1, i_2) + \overline{C}(i_2, i_3) + ... + \overline{C}(i_n, i_1) \geq d(X). \quad (6)$$

Неравенство (6) показывает, что $d(X)$ является оценкой снизу для множества X.

Кроме того, после редукции длины всех маршрутов уменьшаются на одну и ту же величину $d(X)$ и, следовательно, оптимальный маршрут, найденный с использованием редуцированной матрицы $\overline{C}$, оптимален и для исходной задачи. Процесс ветвления при поиске оптимального маршрута можно представить в виде дерева, каждая вершина которого соответствует некоторому множеству маршрутов, являющемуся подмножеством множества X. При этом начальная вершина соответствует множеству всех маршрутов X (рис. 4, [2]).

На каждом шаге из числа кандидатов на ветвление выбирается множество X^1 с наименьшей оценкой. Это множество разделяется на два подмножества X_1^1 и X_2^1. Подмножество X_1^1 состоит из всех маршрутов множества X^1, содержащих некоторую выбранную на данном шаге дугу $(\overline{r,s})$, а подмножество X_2^1 – из всех маршрутов множества X^1, не содержащих дугу (r,s). Общие издержки $Z(x)$ для цикла x определяются через сумму элементов матрицы C по коммуникациям маршрута $Z(x) = \sum_{(i,j) \in x} c_{i,j.}$. Отметим, что в цикле содержатся только один элемент каждой строки и каждого столбца.

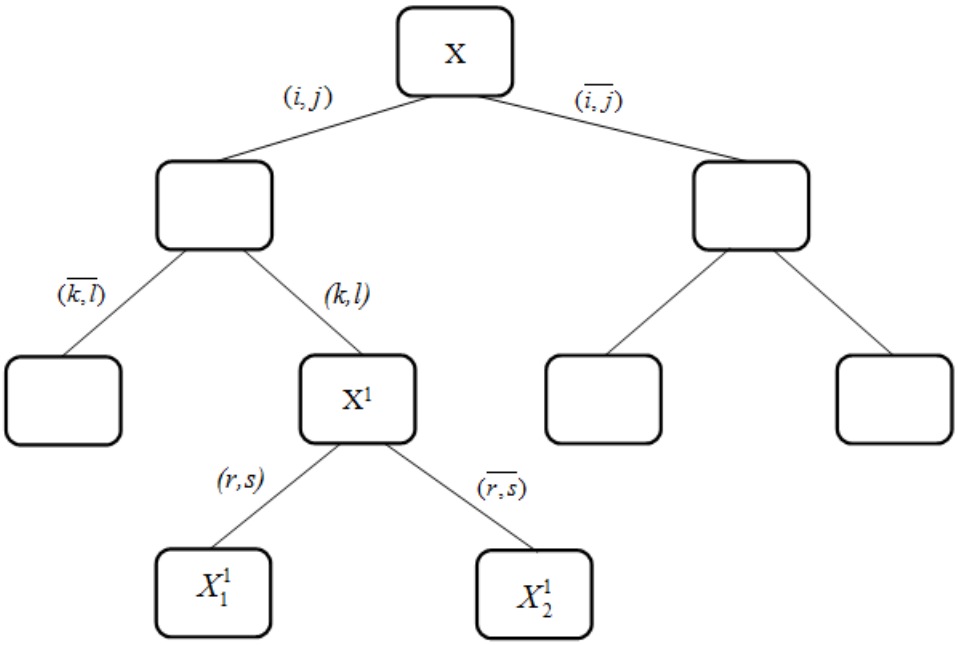

Рис. 4. *Иллюстрация процесса ветвления*

Рассмотрим **вычислительный пример** для случая $m = 6$. Пусть требуется определить оптимальную программу обхода сегментов сетевой модели (рис. 3) для случая $n = m + 1 = 6$ по критерию минимума затрат времени T_Σ, начиная с вершины W_6.

В ходе мониторинга не должны быть превышены допустимые границы потребляемых вычислительных ресурсов $R_\Sigma \le R_{ДОП}$. Исходные данные, необходимые для расчётов, выраженные в относительных единицах, представлены матрицами C и R.

В результате компьютерного решения задачи коммивояжера определена оптимальная (по критерию минимума затрат времени) схема обхода сегментов сети при её активном мониторинге: (6-1) → (1-5) → (5-3) → (3-4) → (4-2) → (2-6). Достигаемые значения показателей эффективности мониторинга приведены в таблице (составлена авторами).

$C =$

	1	2	3	4	5	6
1	∞	8	12	6	5	11
2	14	∞	12	6	4	7
3	7	12	∞	5	8	10
4	8	6	13	∞	10	12
5	5	9	2	4	∞	8
6	9	3	5	7	6	∞

$R =$

	1	2	3	4	5	6
1	∞	4	5	2	8	8
2	7	∞	2	2	9	12
3	8	2	∞	5	3	9
4	5	5	8	∞	20	15
5	3	18	6	10	∞	14
6	2	10	7	9	8	∞

Анализ показал, что несколько лучший результат решения задачи оптимизации по критерию минимума временных затрат $C_\Sigma = 33\ y.e.$ достигается при использовании другой программы мониторинга: (6-2) → (2-5) → (5-3) → (3-4) → (4-1) → (1-6). Однако, указанная программа неприемлема, так как потребляемые при её осуществлении вычислительные ресурсы превышают допустимые ограничения: $R_\Sigma = 43\ y.e. \ge 40\ y.e.$

Таблица

Результаты решения задачи коммивояжера с учётом ограничения $R_{\Sigma} \leq 40$ *у.е.*

Фазы мониторинга						Показатели программы	
6-1	1-5	5-3	3-4	4-2	2-6	T_{Σ}, *у.е.*	R_{Σ}, *у.е.*
9	5	2	5	6	7	34	-
2	8	6	5	5	12	-	38

Разработанные авторами алгоритмы и процедуры сегментации сетевой модели и оптимизации программы мониторинга ресурсов ИВС ОО прошли успешную апробацию в ходе решения ряда прикладных задач. В частности, для контрольного тестирования компьютерной программы, обеспечивающей решение задачи коммивояжера методом ветвей и границ, в качестве контрольных примеров использовались комбинаторные задачи, представленные в известной работе [2].

Как показали наши исследования, обоснованное внедрение средств автоматизации активного мониторинга способно повысить объективность информации, необходимой для управления рисками информационной безопасности ИВС ОО. Результаты мониторинга позволяют не только фиксировать 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 определить потенциального инсайдера и предотвратить несанкционированные действия и возможную утечку конфиденциальной информации.

В целом активный мониторинг следует рассматривать как базовый компонент системы интегрированной защиты ресурсов инфраструктуры ИВС ОО [4]. На его основе могут быть построены гибкие автоматизированные механизмы контроля функционального состояния критических сегментов сети и выявления потенциальных инсайдеров. Это позволит своевременно принимать адекватные организационные меры и корректировать параметры принятой в организации модели разграничения прав доступа.

ЛИТЕРАТУРА

1. Васенин В. А. К созданию средств мониторинга работоспособности элементов Грид-систем / В.А. Васенин, М.А. Занчурин, А.А. Коршунов // Программная инженерия. 2011. – № 6. – С. 36-43.
2. Ляшенко И. Н. Линейное и нелинейное программирование / И.Н. Ляшенко, Е.А. Карагодова, Н.В. Черникова, Н.З. Шор. – Киев : Издат. объединение «Вища школа», 1975. – 372 с.
3. Корнеев В. В. Управление сетевой средой распределенных вычислений / В.В. Корнеев, А.В. Киселев, А.В. Баранов и др. // ФГУП «НИИ «Квант», г. Москва. Режим доступа: http://old.lvk.cs.msu.su/files/mco2003/korneev.pdf , свободный. – Загл. с экрана. – Яз. рус.
4. Надеждин Е. Н. Методы моделирования и оптимизации интегрированных систем управления организационно-технологическими процессами в образовании : монография / Е.Н. Надеждин, Е.Е. Смирнова. – Тула : Изд-во ТулГУ, 2013. – 250 с.
5. Надеждин Е. Н. Математические основы моделирования и анализа интегрированных систем защиты информации : учебное пособие / Е.Н. Надеждин, Е.Е. Смирнова, Т.Л. Шершакова. – Тула : НОУ ВПО «Московский институт комплексной безопасности». Изд-во ТулГУ, 2013. – 206 с.
6. Надеждин Е. Н. Алгоритм декомпозиции сетевой инфраструктуры системы организационного управления / Е.Н. Надеждин, П.В. Допира, Негосударственное образовательное учреждение высшего профессионального образования (институт) «Высшая школа бизнеса, безопасности и управления». – Тула, 2013. – 12 с. 2 ил. – Библиогр. 10 назв. – Русс. – Деп. в ВИНИТИ 03.12.2013 г.; № 352-В2013.
7. Цветков А. А. Сетевая модель активного мониторинга рабочих станций распределенной информационно-вычислительной сети // Информационная среда образования и науки [Электронный ресурс]: Электронное периодическое издание. – М. : ИИО РАО, 2013. Вып. 15. – Режим доступа: http://www.iiorao.ru/iio/pages /izdat/ison/publication/ison_2013/num_15_2013, свободный. – Загл. с экрана. – Яз. рус.
8. Цветков А. А. Обоснование показателей качества активного мониторинга ресурсов информационно-вычислительной сети // Научный поиск, №2.5. 2013. – С. 70-72.
9. Цветков А. А. Идентификация профиля пользователя распределенной вычислительной сети на основе активного мониторинга // Информационная среда образования и науки [Электронный ресурс]: Электронное периодическое издание. – М. : ИИО РАО, 2013. Вып. 17. – Режим доступа: http://www.iiorao.ru/iio /pages/izdat/ison/publication/ison_2013/num_17_2013, свободный. – Загл. с экрана. – Яз. рус.
10. Юдин Д.Б., Гольштейн Е.Г. Линейное программирование. – М. : Наука, 1969. – 424 с.

Рецензент: Логвинов Сергей Иванович, ФГБОУ ВПО «Тульский государственный педагогический университет им. Л.Н. Толского», профессор кафедры экономики и управления, доктор технических наук, профессор.

Yevgeniy Nadezhdin
State Institute of Information Technologies and Telecommunications
Russia, Moscow.
E-Mail: e.nadezhdin@informika.ru

Aleksey Tsvetkov
Shuya branch of Ivanovo State University
Russia, Shuya

The synthesis of the computer network resources monitoring program in educational institution

Abstract. Quick analysis of data about a current status of network resources and unauthorized users actions can be information basis to detect the potential vulnerabilities and computer network insiders, to set up the mechanisms of resource protection and to low the information security risks. In this regard there are actual problems of the active organization and of the intellectual analysis of the data received on monitoring basis. In this paper it is formulated the problem of synthesis of the remote resources monitoring program in the distributed computer network of the educational institution to implement the automated situation-dependent management of information security risks. Thus the problem of synthesis of the remote monitoring program is based on optimization of the diagram of the under control network nodes bypass for achievement the best measure values of resources monitoring efficiency of the distributed computer network. The problem definition of synthesis is transformed to canonical model of the task of the direct-sales representative which was solved by the method of branches and boundaries. Also in the present article there are results of computing experiment where the optimum diagram of the network nodes bypass is defined, this diagram brings to the essential lowering of the time and computing resources expenses that confirms efficiency of the developed technique application.

Keywords: the distributed computer network; educational institution; remote monitoring of resources; the active monitoring of a network; problem of synthesis of the monitoring program; monitoring optimization; task of the direct-sales representative; method of branches and borders; bypass of a computer network nodes; computing experiment.

REFERENCES

1. Vasenin V. A. K sozdaniju sredstv monitoringa rabotosposobnosti jelementov Grid-sistem / V.A. Vasenin, M.A. Zanchurin, A.A. Korshunov // Programmnaja inzhenerija. 2011. – № 6. – S. 36-43.
2. Ljashenko I. N. Linejnoe i nelinejnoe programmirovanie / I.N. Ljashenko, E.A. Karagodova, N.V. Chernikova, N.Z. Shor. – Kiev : Izdat. ob#edinenie «Vishha shkola», 1975. – 372 s.
3. Korneev V. V. Upravlenie setevoj sredoj raspredelennyh vychislenij / V.V. Korneev, A.V. Kiselev, A.V. Baranov i dr. // FGUP «NII «Kvant», g. Moskva. Rezhim dostupa: http://old.lvk.cs.msu.su/files/mco2003/korneev.pdf , svobodnyj. – Zagl. s jekrana. – Jaz. rus.
4. Nadezhdin E. N. Metody modelirovanija i optimizacii integrirovannyh sistem upravlenija organizacionno-tehnologicheskimi processami v obrazovanii : monografija / E.N. Nadezhdin, E.E. Smirnova. – Tula : Izd-vo TulGU, 2013. – 250 s.
5. Nadezhdin E. N. Matematicheskie osnovy modelirovanija i analiza integrirovannyh sistem zashhity informacii : uchebnoe posobie / E.N. Nadezhdin, E.E. Smirnova, T.L. Shershakova. – Tula : NOU VPO «Moskovskij institut kompleksnoj bezopasnosti». Izd-vo TulGU, 2013. – 206 s.
6. Nadezhdin E. N. Algoritm dekompozicii setevoj infrastruktury sistemy organizacionnogo upravlenija / E.N. Nadezhdin, P.V. Dopira, Negosudarstvennoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija (institut) «Vysshaja shkola biznesa, bezopasnosti i upravlenija». – Tula, 2013. – 12 s. 2 il. – Bibliogr. 10 nazv. – Russ. – Dep. v VINITI 03.12.2013 g.; № 352-V2013.
7. Cvetkov A. A. Setevaja model' aktivnogo monitoringa rabochih stancij raspredelennoj informacionno-vychislitel'noj seti // Informacionnaja sreda obrazovanija i nauki [Jelektronnyj resurs]: Jelektronnoe periodicheskoe izdanie. – M. : IIO RAO, 2013. Vyp. 15. – Rezhim dostupa: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2013/num_15_2013, svobodnyj. – Zagl. s jekrana. – Jaz. rus.
8. Cvetkov A. A. Obosnovanie pokazatelej kachestva aktivnogo monitoringa resursov informacionno-vychislitel'noj seti // Nauchnyj poisk, №2.5. 2013. – S. 70-72.
9. Cvetkov A. A. Identifikacija profilja pol'zovatelja raspredelennoj vychislitel'noj seti na osnove aktivnogo monitoringa // Informacionnaja sreda obrazovanija i nauki [Jelektronnyj resurs]: Jelektronnoe periodiche-skoe izdanie. – M. : IIO RAO, 2013. Vyp. 17. – Rezhim dostupa: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2013/num_17_2013, svobodnyj. – Zagl. s jekrana. – Jaz. rus.
10. Judin D.B., Gol'shtejn E.G. Linejnoe programmirovanie. – M. : Nauka, 1969. – 424 s.