ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

2

(81)

В НОМЕРЕ

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2008

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

2

(81)

В НОМЕРЕ

Подписывайтесь,
читайте,
пишите в наш журнал

Москва 2008

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
"ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МЕЖОТРАСЛЕВОЙ ИНФОРМАЦИИ — ФЕДЕРАЛЬНЫЙ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР
ОБОРОННОЙ ПРОМЫШЛЕННОСТИ" (ФГУП "ВИМИ")

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

2 (81)

Москва
2008
Основан
в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн./ФГУП "ВИМИ", 2008. Вып. 2 (81). С. 1—60.

Редакторы: *Л. К. Андрианова, М. С. Куприенко*
Корректор *Н. С. Кузьмина*
Компьютерная верстка *Н. В. Соколова*

Подписано в печать 07.05.2008.
Формат 60x84 1/8.
Бумага офсетная. Печать офсетная. Усл. печ. л. 7,0.
Уч.-изд. л. 7,8. Тираж 500 экз.
Заказ 1468. Цена договорная.
Отпечатано в ФГУП "ВИМИ".
125993, Москва.
E-mail: office@vimi.ru
http://infogoz.vimi.ru/main_izd.php
Индекс 79187.

УДК 681.5

Метод вычисления вероятности отказоустойчивости и надежности информационной системы "Население и миграция"

Ф. Д. Абдуллаева

Предложен метод вычисления отказоустойчивости и надежности распределенной информационной системы (ИС) "Население и миграция". Отказы серверов ИС "Население и миграция", являющихся независимыми один от другого, моделируются как распределение Пуассона с интенсивностью λ. Для вычисления отказоустойчивости и надежности использован способ резервируемости объектов. Резервирование в данном случае выглядит как перенаправление повторных запросов пользователей на альтернативный сервер. Проведен численный расчет вычисления вероятности отказоустойчивости ИС "Население и миграция".

Современный уровень развития вычислительных средств и широкое их внедрение во все области деятельности человека все более требуют создания ИС с высоким уровнем надежности и отказоустойчивости.

Высокая отказоустойчивость ИС может достигаться при их резервировании, предусматривающем перераспределение запросов отказывающих вычислительных узлов на исправные [1–3].

Резервирование — один из основных методов повышения надежности, который позволяет по крайней мере в принципе безгранично повышать надежность и отказоустойчивость систем [4].

Исследованию отказоустойчивости и надежности посвящено большое число работ. Условия размещения ресурсов по узлам отказоустойчивых вычислительных систем, динамического распределения запросов при ограничении числа узлов, методы оценки вероятности безотказной работы систем с рациональным размещением ресурсов и оценки их отказоустойчивости предложены в работах В. А. Богатырева [5]. Оптимизационная модель отказоустойчивости виртуальных частных сетей (VPN) при аутентификации авторизованных пользователей предложена в работе [6]. Метод отказоустойчивости, статически распределяющий множество независимых задач, предназначенный только для однородных систем, предложен в [7].

Надежность и отказоустойчивость систем с резервированием при неоднородности ИС и с распределением запросов независимых друг от друга к настоящему времени не изучены. В предлагаемой статье рассмотрена неоднородная ИС с распределенной архитектурой, которая широко распространена в настоящее время.

Постановка задачи

Существует много способов обеспечения отказоустойчивости и надежности ИС. Спецификация отказоустойчивости ИС "Население и миграция", являясь компромиссом для многочисленных решений в этой области, регламентирует такие аспекты, как резервируемость, обнаружение отказа и восстановление.

Способом достижения резервируемости избрано перенаправление запросов пользователей на альтернативный сервер, имеющий работоспособное состояние.

Рассмотрим ИС "Население и миграция", состоящую из $P = P_i \,|\, i = \overline{1,n}$ серверов, каждая из которых обрабатывает в исходном состоянии $V = \{v_1, v_2, \ldots, v_n\}$ запросов.

Информационная система может находиться в одном из состояний:

полной работоспособности (с возможностью обрабатывать все запросы) $V = \{v_1, v_2, \ldots, v_n\}$;

частичной работоспособности;

полного отказа.

Отказы серверов системы будем считать независимыми. Суть задачи заключается в том, что администратор безопасности ИС при отказах некоторых серверов распределяет запросы по работоспособным серверам. Требуется оценить отказоустойчивость и надежность ИС "Население и миграция".

Метод вычисления отказоустойчивости и надежности

Учитывая, что под резервированием в данном случае понимается перенаправление повторных запросов пользователей на альтернативный сервер, функционирование ИС "Население и миграция" будем моделировать направленным ациклическим графом $T = \{V, E\}$, где E — множество граней, представляющих связь между запросами, $e_{ij} = (v_i, v_j) \in E$

указывает задание, переданное от запроса v_i к запросу v_j. К отказам в одном сервере применятся основная – резервная методика [4]. Для того чтобы обеспечить отказоустойчивость ИС, каждый запрос имеет основную и резервную копии, обозначенные как v^P и v^B и выполненные последовательно на двух различных серверах.

Информационная система "Население и миграция" состоит из множества $P=\{p_1,p_2,\ldots,p_m\}$ разнородных серверов, связанных сетью. Кроме того, в гетерогенных распределенных системах каждый запрос v_i имеет различное время выполнения на различных серверах. $C: V\times P\to Z^+$ представляет время выполнения каждого запроса на каждом сервере. Таким образом, $c_j(v_i)$ показывает время выполнения запроса v_i на сервере p_j.

Время связи отправки сообщения e от v_s, расположенного на сервере p_i, к v_r, расположенного на сервере p_j, определяется как $M: E\times P\times P\to Z^+$; $p(v)$ показывает сервер, в котором расположен запрос v.

При большом числе испытаний, в каждом из которых вероятность события очень мала, для определения вероятности появлений события в этих испытаниях используют распределение Пуассона [8]. Как известно, процессом Пуассона описывают математические модели редких событий, и он широко применяется в прикладных областях для построения стохастических моделей сложных систем [9]. Принимая это во внимание, можно сказать, что отказы серверов информационной системы "Население и миграция", являющихся независимыми один от другого, подчиняются распределению Пуассона с интенсивностью λ. Таким образом, вероятность n событий в течение временного интервала t по распределению Пуассона имеет вид

$$\Pr_n(t)=\frac{e^{-\lambda t}(\lambda t)^n}{n!}.$$

Предположим, что K – случайная величина для числа отказов и $F_i(t)$ является вероятностью того, что p_i не откажет во время t. В этом случае $F_i(t)$ выражается следующим равенством:

$$F_i(t)=\Pr[K=0]=e^{-\lambda_i t}, \qquad (1)$$

где $\lambda_i\,(1\le i\le m)$ – интенсивность отказов p_i в векторе $R=(\lambda_1,\lambda_2,\ldots,\lambda_m)$. Состояние системы представляется случайной переменной X, которая принимает значения $\{0,1,2,\ldots,m\}$. Более точно $X=0$ означает, что постоянно никакой сервер не отказывает и $X=i\,(1\le i\le m)$ показывает, что p_i постоянно сталкивается с отказом. Вероятность для X определяется следующим равенством:

$$\Pr[X=x]=\begin{cases}\prod_{i=1}^{m}F_i(t_i)=\prod_{i=1}^{m}e^{-\lambda_i t_i}-\text{для } x=0,\\ (1-F_i(t_i))\prod_{j=1,j\ne i}^{m}F_j(t_j)=\left(1-e^{-\lambda_i t_i}\right)\times\\ \times\prod_{j=1,j\ne i}^{m}e^{-\lambda_j t_j}-\text{для } x=i,(1\le i\le m).\end{cases} \qquad (2)$$

Отказоустойчивость тесно связана с понятием надежности [4, 10]. Надежность ИС можно моделировать как произведение λ_j интенсивности p_j на время выполнения запросов v_i в сервере p_j. С этой точки зрения допустим, что $N(P)$ является значением надежности данной системы. Согласно предположению, что не больше чем один сервер постоянно отказывает, т. е. $\sum_{i=0}^{m}\Pr(X=i)=1.$, среднее значение величины $N(P)$ можно выразить в виде

$$E(N(P))=\sum_{i=0}^{m}\left(N_i(P)\times\Pr[X=i]\right), \qquad (3)$$

где $N_0(P)$ – значение надежности, когда никакой сервер не отказывает, и $N_i(P)(1\le i\le m)$ – значение надежности, когда p_i отказывает.

N_0 и N_i определяются равенствами:

$$N_0(P)=\sum_{i=1}^{m}\sum_{p(v^P)=i}\lambda_i c_i(v); \qquad (4)$$

$$N_i(P)=\sum_{j=1,j\ne i}^{m}\sum_{p(v^P)=j}\lambda_j c_j(v)+$$

$$+\sum_{j=1,j\ne i}^{m}\sum_{p(v^P)=i,p(v^B)=j}\lambda_j c_j(v)=\sum_{j=1,j\ne i}^{m}\times$$

$$\times\left(\sum_{p(v^P)=j}\lambda_j c_j(v)+\sum_{p(v^P)=i,p(v^B)=j}\lambda_j c_j(v)\right). \qquad (5)$$

В равенстве (5) первое слагаемое в правой части представляет собой надежность, состоящую из запросов, основные копии которых расположены на неотказывающих серверах, в то время как вторая сумма выражает надежность, состоящую из резервных копий запросов, основные копии которых расположены на отказанном сервере. Используя уравнения (3)–(5), получим среднее значение надежности в виде

$$E(N(P))=N_0(P)\prod_{i=1}^{m}e^{-\lambda_i\tau_i}+$$

$$+\sum_{i=0}^{m}\left[N_i(P)\left(1-e^{-\lambda_i\tau_i}\right)\prod_{j=1,j\ne i}^{m}e^{-\lambda_j\tau_j}\right]. \qquad (6)$$

Таким образом, предложена модель обеспечения отказоустойчивости и надежности неоднородной распределенной ИС "Население и миграция" с резервированием, предусматривающим перераспределение запросов. Предложенный метод по сравнению с разработанными методами имеет преимущество в том, что он рассчитан на оценку отказоустойчивости и надежности неоднородных распределенных систем.

Все серверы в гетерогенных распределенных системах имеют различные интенсивности, и каждый запрос имеет различное время выполнения в различных серверах.

Замечание 1. В частном случае, когда система является однородной, $\lambda_1 = \lambda_2 = \ldots = \lambda_m = \ldots = \lambda$, и полагая $t_1 = t_2 = \ldots = t_m = t$, из (2) имеем:

$$P_r(X = 0) = e^{-m\lambda t},$$

и для i, $1 \le i \le m$ имеем:

$$P_r(X = i) = \left(1 - e^{-\lambda t}\right) e^{-(m-1)\lambda t}.$$

В этом случае формула (6) имеет вид

$$E(N(P)) = N_0(P)e^{-m\lambda t} + \left(1 - e^{-\lambda t}\right)e^{(m-1)\lambda t}\sum_{i=0}^{N} N_i(P).$$

Замечание 2. В случае $t_1 = t_2 = \ldots = t_m = t$ для неоднородной системы формула (2) принимает вид

$$P_r(X = 0) = e^{-t\sum_{i=1}^{m}\lambda_i},$$

и для i, $1 \le i \le m$ имеем

$$P_r(X = i) = (1 - e^{-\lambda_i t})e^{-t\sum_{j=1, i\ne j}^{m}\lambda_j}.$$

Рассмотрим пример использования приведенных равенств для вычисления вероятности отказоустойчивости ИС "Население и миграция".

В практических задачах интенсивность отказов обычно принимает различные значения, например, $m = 5$; $\lambda_1 = 0{,}9$; $\lambda_2 = 0{,}95$; $\lambda_3 = 1$; $\lambda_4 = 1{,}05$; $\lambda_5 = 1{,}10$ [11].

Предположим, что время t дискретно и принимает значения $t_1 = t_2 = \ldots = t_m = 1$, тогда в силу замечания 2 находим, что

$$P_r(X = 0) = e^{-\sum_{i=1}^{m}\lambda_i} = e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4+\lambda_5)} =$$
$$= e^{-5} = 2{,}71^{-5} = \frac{1}{2{,}71^5} \approx \frac{1}{146{,}166} \approx 0{,}007.$$

$$P_r(X = 1) = \left(1 - e^{-\lambda_1}\right)e^{-(\lambda_2+\lambda_3+\lambda_4+\lambda_5)} =$$
$$= \left(1 - e^{-0{,}9}\right)e^{-4{,}1} = \left(1 - 2{,}71^{-0{,}9}\right)\times 2{,}71^{-4{,}1} =$$
$$= \left(1 - \frac{1}{2{,}71^{0{,}9}}\right)\frac{1}{2{,}71^{4{,}1}} \approx \left(1 - \frac{1}{2{,}453}\right)\frac{1}{59{,}590} \approx$$
$$\approx (1 - 0{,}408)0{,}017 \approx 0{,}592\times 0{,}017 \approx 0{,}010064;$$

$$P_r(X = 2) = \left(1 - e^{-\lambda_2}\right)e^{-(\lambda_1+\lambda_3+\lambda_4+\lambda_5)} =$$
$$= \left(1 - e^{-0{,}05}\right)e^{-4{,}05} = \left(1 - \frac{1}{e^{0{,}05}}\right)\frac{1}{e^{4{,}05}} =$$
$$= \left(1 - \frac{1}{2{,}71^{0{,}05}}\right)\frac{1}{2{,}71^{4{,}05}} \approx \left(1 - \frac{1}{1{,}051}\right)\frac{1}{56{,}693} \approx$$
$$\approx (1 - 0{,}951)\times 0{,}018 \approx 0{,}049\times 0{,}018 \approx 0{,}000882;$$

$$P_r(X = 3) = (1 - e^{-\lambda_3})e^{-(\lambda_1+\lambda_2+\lambda_4+\lambda_5)} =$$
$$= (1 - e^{-1})e^{-4} = \left(1 - 2{,}71^{-1}\right)\times 2{,}71^{-4} =$$
$$= \left(1 - \frac{1}{2{,}71}\right)\frac{1}{2{,}71^4} \approx 0{,}631\times 0{,}019 \approx 0{,}011989;$$

$$P_r(X = 4) = (1 - e^{-\lambda_4})e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_5)} =$$
$$= (1 - e^{-1{,}05})e^{-3{,}95} = \left(1 - 2{,}71^{-1{,}05}\right)\times 2{,}71^{-3{,}95} =$$
$$= \left(1 - \frac{1}{2{,}71^{1{,}05}}\right)\frac{1}{2{,}71^{3{,}95}} \approx \left(1 - \frac{1}{2{,}849}\right)\frac{1}{51{,}313} \approx$$
$$\approx (1 - 0{,}351)\times 1{,}949 \approx 0{,}649\times 1{,}949 \approx 1{,}265;$$

$$P_r(X = 5) = (1 - e^{-\lambda_5})e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)} =$$
$$= (1 - e^{-1{,}1})e^{-3{,}9} = \left(1 - 2{,}71^{-1{,}1}\right)\times 2{,}71^{-3{,}9} =$$
$$= \left(1 - \frac{1}{2{,}71^{1{,}1}}\right)\frac{1}{2{,}71^{3{,}9}} \approx \left(1 - \frac{1}{2{,}994}\right)\frac{1}{48{,}818} \approx$$
$$\approx (1 - 0{,}334)\times 0{,}02 \approx 0{,}666\times 0{,}02 \approx 0{,}01332.$$

Отметим, что если в рассматриваемом случае известны значения надежности $N_0(P)$; $N_1(P)$; $N_2(P)$; $N_3(P)$; $N_4(P)$ и $N_5(P)$, то среднее значение надежности информационной системы будем вычислять по формуле (3) или (6).

Заключение

В работе предложен метод вычисления отказоустойчивости и надежности гетерогенной распределенной системы "Население и миграция".

Все серверы в гетерогенных распределенных системах имеют различные интенсивности, и каждый запрос имеет различное время выполнения в различных серверах.

Для вычисления отказоустойчивости и надежности использован способ резервируемости объектов. Резервирование в данном случае выглядит как перенаправление повторных запросов пользователей на альтернативный сервер.

Литература

1. *Бернер Л. И.* Подсистема динамического перераспределения задач отказавших узлов распределенных АСУТП// Приборы и системы управления. 1991. № 12. С. 5–6.

2. *Денисов С. Г., Турута Е. Н.* Восстановление вычислительных процессов в многомашинной системе на основе их

реактивации// Управление ресурсами в интегральных сетях. — М.: Наука, 1991. С. 117—129.

3. *Симоненко В. П.* Модель распределения задач в неоднородных системах распределенной обработки данных// Электронное моделирование. 1998. Т. 20. № 1. С. 44—55.

4. *Гнеденко Б. В., Беляев Ю. К. Соловьев А. Д.* Математические методы в теории надежности. — М.: Наука, 1965.

5. *Богатырев В. А.* К оценке отказоустойчивости вычислительных систем с учетом размещения функциональных ресурсов// Информационные технологии. 2000. № 7. С. 9—13.

6. *Алгулиев Р. М.* Алгоритм обеспечения отказоустойчивости VPN// Автоматизация проектирования, № 2// Издательство "Открытые системы". 1999, http://www.osp.ru/ap/1999/ 02/008.htm

7. *Oh Y., Son S. H.* Scheduling real-time tasks for dependability// Journal of operational research society. 1997. V. 48. № 6. P. 629—639.

8. *Гмурман В. Е.* Теория вероятностей и математическая статистика. Изд. 4-е, доп.: Учеб. пособие для вузов. — М.: Высш. шк., 1972. — 368 с.

9. *Штойян Д.* Качественные свойства и оценки стохастических моделей// Пер. с нем. — М.: Мир, 1979. — 269 с.

10. *Kopetz H., Verissimo P.* Real Time and Dependability Concepts. In Mullender S., Distributed Systems. P. 411—446. Wokingham: Addison-Wesley, 1993.

11. *Srinivasan S., Jha N. K.* Safety and Reliability Driven Task Allocation in Distributed Systems// IEEE Transactions on Parallel and Distributed Systems. 1999. V. 10. № 3.

УДК 681.3:002.5

Полуформальные модели стандартов информационной безопасности

А. В. Любимов, канд. техн. наук;
А. В. Суханов, канд. техн. наук

В статье предлагается обобщенный подход к постановке и решению ряда задач информационной безопасности (ИБ), основанный на разработке систем согласованных полуформальных моделей стандартов, существующих в данной предметной области. В рамках подхода формулируется и решается задача построения библиотеки объектных и процессных моделей, определяются области ее текущего и перспективного применения, приводится ряд конкретных актуальных практических задач информационной безопасности, решаемых с ее использованием. Возможности подхода иллюстрируются двумя примерами: выявление методологии стандарта путем его объектного анализа, а также дополнение и коррекция стандарта на основе его процессной модели.

Постановка задачи и подход к исследованию

Одной из важных проблем информационной безопасности численно возрастающих разнородных стандартов является проблема согласования, гибридизации и взаимоучета методологий (методик) в этой области. Эффективное решение этой проблемы возможно лишь на основе подхода, позволяющего строить для этих методологий универсальные представления, которые могли бы служить базой для принятия решений и практических разработок. В качестве такого подхода предлагается использовать хорошо себя зарекомендовавшие и имеющие широкую аналитическую и инструментальную поддержку методы полуформального моделирования.

В данной работе в качестве предметной области исследования выбраны следующие линейки стандартов ИБ: линейка общих критериев (ОК), содержащая общие критерии и методологию оценивания безопасности информационных технологий (ИТ); линейка стандартов ISO 2700x, трактующих вопросы построения и использования системы управления информационной безопасностью (СУИБ) организации, линейка руководящих документов ФСТЭК РФ, а также некоторые отраслевые стандарты ИБ (например стандарт ЦБ РФ). Предлагаемый в работе подход и используемые методы допускают включение в предметную область любых других стандартов ИБ, например, ведомственных и корпоративных. Выбор именно стандартов как объектов исследования представляется важным в первую очередь по той причине, что в большинстве своем они содержат обобщение накопленного в предметной области и получившего широкое признание опыта, причем представленного в сжатой и определенным образом структурированной форме.

При сформулированном подходе основным методом исследования является построение связанной системы структурных моделей каждого стандарта и линейки в целом. Под структурной моделью далее понимается либо процессная модель, описывающая функциональную структуру предметной области и использующая в качестве основных компонентов понятия процесса и потока ресурсов, либо объектная модель, описывающая онтологическую структуру предметной области и использующая в качестве основных компонентов понятия класса и отношения. Понимаемые таким образом структурные модели относятся к классу