

УДК 004.519.217

Д.А. МАЕВСКИЙ

Одесский национальный политехнический университет, Украина

ОЦЕНКА ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ МНОГОКОМПОНЕНТНЫХ ПРОГРАММНЫХ СИСТЕМ

В работе проведено расширение теории динамики программных систем на случай WEB и Cloud-систем, имеющих многокомпонентную структуру. Рассмотрены потоки дефектов в многокомпонентных системах и их взаимные влияния на основе принципов равновесия, взаимности и суперпозиции. Получена математическая модель процесса выявления дефектов многокомпонентных систем в виде автономной системы дифференциальных уравнений. Модель описывает взаимодействие потоков дефектов и позволяет спрогнозировать количество дефектов в системе в любой момент времени. Поэтому созданную модель можно рассматривать как модель надежности многокомпонентных программных систем. На примере двухкомпонентной системы без учета вторичных дефектов объяснено ранее отмеченное явление внутреннего равновесия программных систем.

Ключевые слова: многокомпонентная система, модель надежности, динамика программных систем, программные дефекты, потоки дефектов.

Введение

Проблема обеспечения и прогнозирования надежности программного обеспечения информационных систем является одной из наиболее актуальных проблем современной программной инженерии. Особенно это относится к сложным программным системам (ПС), имеющим многокомпонентную структуру. К таким многокомпонентным системам относятся практически все WEB и Cloud-сервисы, в состав которых входит большое количество самостоятельных программных систем, часто работающих на разных платформах и физически размещающихся на разных компьютерах. Так, например, реализуемый в Cloud-сервисах подход «инфраструктура как услуга» («Infrastructure-as-a-Service», IaaS) предполагает предоставление в распоряжение пользователя различное взаимодействующее программное обеспечение, такое как операционные системы, прикладные программы, системы управления базами данных и другие. Для организации взаимодействия используемых компонент используется специализированное промежуточное программное обеспечение (ПО), обеспечивающее мониторинг состояния оборудования и программ, перераспределение нагрузки и обеспечение ресурсов для решения требуемой задачи.

Таким образом, появление сетевых технологий неизбежно приводит к необходимости использования многокомпонентных программных систем, от надежности функционирования которых зависят жизнь и благополучие человека в современном обществе. Любой отказ таких систем неизбежно при-

водит к негативным последствиям. Эти последствия сегодня могут быть любыми – от легкой неприятности из-за заблокированного прохода на эскалатор до проблем масштаба Чернобыля или отказов систем управления важными объектами – транспорт, связь, энергетика. Поэтому обеспечение надежности многокомпонентных программных систем, разработка методов ее контроля и прогнозирования являются задачей, актуальность решения которой будет расти со временем.

Современное состояние проблемы

Теория надежности программного обеспечения изначально развивалась как часть общей теории надежности технических систем и унаследовала от нее основной математический аппарат – теорию вероятностей. При этом считалось, что отказы программных систем являются, во-первых случайными, а, во-вторых – независимыми событиями. Однако специфика программного обеспечения позволяет оспорить и то и другое предположения. Действительно, как отмечалось многими авторами [1 – 3], отказы программного обеспечения не всегда могут считаться случайными событиями. При повторении одних и тех же условий (набора входных данных) один раз обнаруженный отказ ПО будет повторяться. Этот факт говорит о том, что процесс выявления дефектов не может считаться случайным.

В технике независимость отказов подразумевает, что отказ, проявившийся в одном образце какого-либо изделия, не обязательно проявится в другом. В программных системах дело обстоит как раз

наоборот. Все экземпляры программы, являются полными клонами друг друга. Поэтому отказ, зафиксированный в одном экземпляре, неизбежно повторится и в другом при повторении тех же начальных условий (входных данных), то есть отказы не являются независимыми.

Это свидетельствует о том, что теория вероятностей, так хорошо зарекомендовавшая себя в технических системах, является неприменимой для систем программных. Именно поэтому, по образному выражению И.А. Ушакова [2], попытки уложить надежность ПО в прокрустово ложе теории надежности технических систем, предпринятые при создании моделей надежности ПО, не привели к желаемым результатам. На основании изложенного, в работах [4, 5, 6] предложен детерминированный подход к проблеме надежности ПО на основе теории динамики программных систем (ДПС). Теория ДПС рассматривает программную систему как открытую систему, взаимодействующей с своей внешней средой по законам неравновесных процессов. Исправление (удаление) из ПО дефектов и внесение в него новых вторичных рассматривается как результат действия выходного и входного потоков дефектов. Разработанная на базе теории ДПС математическая модель надежности обеспечивает стабильно точные результаты для всех исследованных программных систем, причем точность оценивания надежности в среднем в 2,5 раза выше наилучшего результата, показанного вероятностными моделями [4]. Поэтому представляет интерес обобщение теории ДПС на многокомпонентную ПС.

Потоки дефектов в многокомпонентной программной системе

Рассмотрим программную систему, состоящую из n относительно независимых компонент. Каждая из компонент выполняет свой определенный набор функций, реализованных в ее программном коде. Относительная независимость компонент предполагает, что они не являются полностью изолированными друг от друга, а могут использовать для решения своих задач общие программные модули. Кроме того, данные полученные в одной компоненте могут быть использованы в других. Таким образом, между программными модулями отдельных компонент существуют связи по управлению и по данным, благодаря которым упомянутые компоненты образуют целостную систему более высокого уровня.

В основу теории динамики многокомпонентных ПС положены следующие принципы.

1. Принцип равновесия. Любая ПС, содержащая дефекты, стремится к равновесию со своей окружающей средой.

2. Принцип взаимности. Все потоки, действующие в ПС, оказывают взаимные влияния друг на друга.

3. Принцип суперпозиции. Одинаково направленные потоки усиливают действие друг друга, а разнонаправленные – ослабляют.

Из принципа равновесия следует существование потоков дефектов, направленных либо из ПС в окружающую среду (первичные дефекты), либо наоборот, из окружающей среды в ПС (вторичные дефекты). При выявлении дефекта в программной компоненте он исправляется, исчезая из нее. Этот процесс можно представить как результат действия выходного потока дефектов, направленного из компоненты в окружающую среду. При исправлении возможно внесение вторичных дефектов, что может быть рассмотрено как результат действия второго, встречно направленного потока – из окружающей среды в программную компоненту.

Законы развития потоков дефектов во времени подобны законам переноса, действующим во всех системах. Согласно теории переноса, в программных системах интенсивность (скорость изменения потока во времени) пропорциональна количеству дефектов, образующих поток. Равновесие между ПС и окружающей средой достигается в тот момент, когда количество дефектов в ПС становится равным нулю. Уменьшающееся со временем количество дефектов в ПС соответствует отрицательной интенсивности соответствующего потока, как производной убывающей функции. В существующих моделях надежности ПС это явление называется возрастанием надежности (*reliability grows*).

Таким образом, с каждой из программных компонент системы связаны два разнонаправленных потока дефектов, поэтому в программной системе в целом действуют $2 \cdot n$ потоков. Обозначим дефекты, образующие потоки как f_1 и f_2 для первой компоненты, f_3 и f_4 для второй и f_{2n-1} , f_{2n} – для n -ной. При этом нечетные номера присвоены потокам выходным потокам, а четные – входным.

Согласно принципу взаимности, эти потоки не существуют обособленно друг от друга, а находятся под влиянием взаимных воздействий – каждый поток влияет на все остальные потоки в системе и одновременно испытывает влияния всех этих потоков. Степень влияния потоков друг на друга будем характеризовать постоянными для данной системы коэффициентами влияния, обозначаемые как A_{ij} . Здесь второй индекс (j) показывает номер влияющего потока (дефектов, образующих влияющий поток), а первый индекс (i) – номер потока, на интенсивность которого оказывается влияние. Например, коэффициент A_{13} определяет степень влияния де-

фектов, образующих поток с номером 3 (выходной поток второй компоненты) на интенсивность потока с номером 1 (выходной поток первой компоненты). Назовем такие коэффициенты взаимными коэффициентами влияния. Согласно принципу Онзагера взаимные влияния потоков одинаковы, т.е. $A_{ij} = A_{ji}$. Коэффициенты с совпадающими индексами (A_{11}, A_{22} и т.д.) назовем собственными коэффициентами влияния. Они являются коэффициентом пропорциональности между количеством дефектов, образующих данный поток и интенсивностью этого потока.

Принцип суперпозиции устанавливает усиление друг другом однонаправленных потоков и ослабление разнонаправленных. В силу этого, коэффициенты влияния однонаправленных потоков (у которых оба индекса или четные или нечетные) будут положительными, а разнонаправленных (четный и нечетный индексы) – отрицательными.

В качестве математической модели взаимодействующих потоков дефектов, согласно теории неравновесных процессов (теории переноса) и принятым допущениям, является следующая система автономных дифференциальных уравнений:

$$\begin{cases} -\frac{df_1}{dt} = A_{11}f_1 - A_{12}f_2 + \dots - A_{1,2n}f_{2n}; \\ -\frac{df_2}{dt} = -A_{21}f_1 + A_{22}f_2 - \dots + A_{2,2n}f_{2n}; \\ \dots \\ -\frac{df_{2n}}{dt} = -A_{2n,1}f_1 + A_{2n,2}f_2 - \dots + A_{2n,2n}f_{2n}. \end{cases} \quad (1)$$

Аналитическое решение системы (1) в общем виде зачастую невозможно, поэтому для получения зависимости количества дефектов в компонентах от времени следует использовать численные методы. Аналитическое решение можно провести для упрощенного случая двухкомпонентной системы.

Потоки дефектов в двухкомпонентной программной системе

Структура двухкомпонентной системы и потоки в ней показаны на рис. 1. Будем полагать, что входные потоки дефектов (потоки вторичных дефектов f_2 и f_4) отсутствуют. При этом математическая модель потоков дефектов упрощается до системы двух дифференциальных уравнений (2):

$$\begin{cases} -\frac{df_1}{dt} = +A_{11} \cdot f_1 + A_{13} \cdot f_3; \\ -\frac{df_3}{dt} = +A_{31} \cdot f_1 + A_{33} \cdot f_3. \end{cases} \quad (2)$$

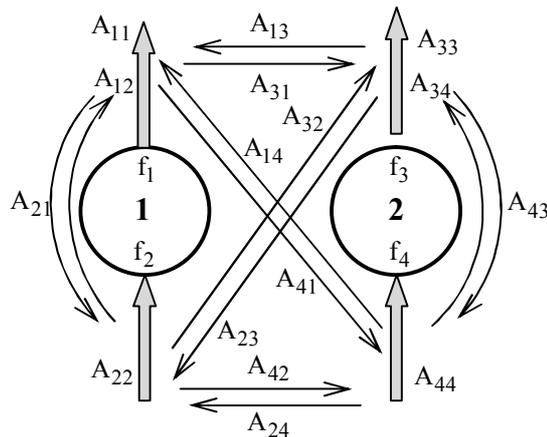


Рис. 2. Потоки в двухкомпонентной программной системе

Знаки перед коэффициентами влияния в системе (2) отражают тот факт, что одинаково направленные (выходные) потоки, согласно принципу суперпозиции, усиливают друг друга.

Решая систему (2) относительно количества дефектов, образующих выходной поток первой компоненты, получаем:

$$f_1(t) = F_{10}e^{-\alpha t} \cdot \left(\text{ch}\beta t + \frac{A_{33} - A_{11}}{2\beta} \text{sh}\beta t \right) - F_{30}e^{-\alpha t} \cdot \frac{A_{13}}{\beta} \text{sh}\beta t. \quad (3)$$

Для количества дефектов выходного потока второй компоненты:

$$f_3(t) = F_{30}e^{-\alpha t} \cdot \left(\text{ch}\beta t + \frac{A_{11} - A_{33}}{2\beta} \text{sh}\beta t \right) - F_{10}e^{-\alpha t} \cdot \frac{A_{31}}{\beta} \text{sh}\beta t. \quad (4)$$

В этих формулах: F_{10} и F_{30} – начальное количество дефектов в первой и третьей компонентах при $t = 0$,

$$\alpha = \frac{A_{11} + A_{33}}{2},$$

$$\beta = \frac{\sqrt{(A_{11} - A_{33})^2 + 4A_{13}A_{31}}}{2}.$$

Рассмотрим частный случай системы с двумя одинаковыми компонентами, одна из которых (для определенности, первая) в начальный момент времени имеет определенное число дефектов, а вторая, подобная первой по структуре и частоте обращений от дефектов свободна. В этом случае имеем: $F_{30} = 0; A_{11} = A_{33} = A_1; A_{13} = A_{31} = A_2$. С учетом этих обозначений коэффициенты α и β значительно упрощаются: $\alpha = A_1, \beta = A_2$ и выражения (3) и (4) могут быть переписаны как

$$f_1 = F_{10}e^{-A_1t} \cdot \text{ch } A_2t, \quad (5)$$

$$f_3 = -F_{10}e^{-A_1t} \cdot \text{sh } A_2t. \quad (6)$$

Обращает на себя внимание то факт, что уравнения (5) и (6) практически полностью совпадают с уравнениями, полученными в теории динамики программных систем для однокомпонентной системы с учетом выходного потока вторичных дефектов. Более того, наличие знака «минус» в уравнении (6) говорит о том, что поток F_3 второй компоненты изменяет свое направление на противоположное, то есть является выходным потоком этой компоненты! Поэтому этот поток может рассматриваться как поток вторичных дефектов, направленный только во вторую компоненту.

Таким образом, можно сделать вывод о том, что поток вторичных дефектов в однокомпонентной системе можно приписать наличию в ней еще одной, реально не существующей «виртуальной» компоненты, ответственной только за создание этого потока. Кроме того, теория двухкомпонентных ПС позволила объяснить еще один, ранее не объясненный факт. В теории ДПС доказывается существование в любой программной системе явления внутреннего равновесия, которое заключается в том, что с течением времени количество дефектов, образующий выходной поток и количество дефектов, внесенных входным потоком (вторичных дефектов) сначала уравниваются, а уже потом синхронно уменьшаются. Это факт хорошо виден на рис. 2 (приведено на основании [4], рис. 9.2, стр. 67).

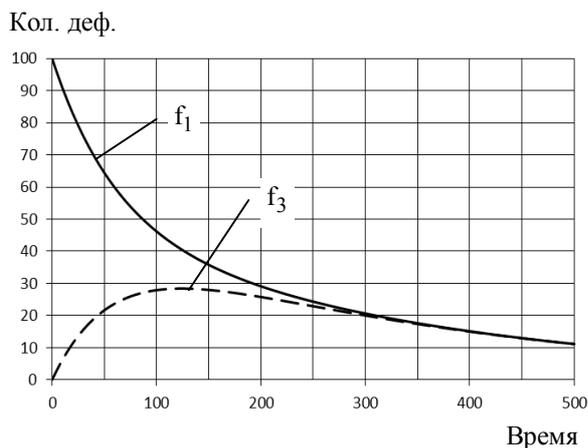


Рис. 2. Иллюстрация явления внутреннего равновесия

Теория динамики программных систем позволяет выявить факт существования явления внутреннего равновесия программных систем, но не позволяет дать ему какую-либо физическую интерпретацию. Однако, введение согласно теории многокомпонентных систем отдельной виртуальной компо-

ненты, ответственной только за возникновение потока вторичных дефектов, позволяет объяснить это явление. Для этого рассмотрим процесс взаимодействия компонент, показанный на рис. 3.

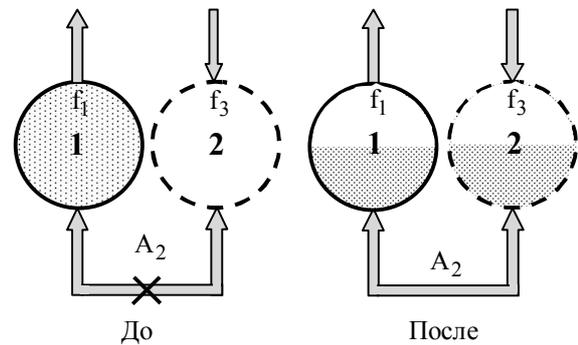


Рис. 3. Программная система до и после наступления состояния равновесия

До начала процесса выявления дефектов компонента 1 (собственно рассматриваемая ПС) содержала какое-то количество дефектов (показано штриховкой). Вторичных дефектов к этому времени существовать не могло, поэтому во второй, виртуальной компоненте, их не было. В это время потоков дефектов еще не существовало, а связь между компонентами отсутствовала. После начала процесса возникли потоки дефектов, обуславливающие появление канала связи между ними (на рисунке обозначен как поток с коэффициентом влияния A_2). Благодаря открытию этого канала связи основная и виртуальная компоненты образуют своеобразную систему «сообщающихся сосудов», что должно привести к уравниванию количества дефектов в обеих компонентах. Однако вспомним, что дефекты в виртуальной компоненте являются вторичными дефектами, количество которых уравнивается с «первичными» дефектами основной компоненты. Поэтому модель на рис. 3 объясняет возникновение явления внутреннего равновесия в программных системах.

Выводы

В работе показано, что теория динамики программных систем может быть распространена на случай систем, состоящих из нескольких компонент, и позволяет прогнозировать процесс выявления дефектов в такой многокомпонентной системе. На основе теории многокомпонентности получило объяснение явление внутреннего равновесия, существование которого было предсказано в теории динамики программных систем. Для практического использования полученных результатов должны быть разработаны методы экспериментального получения коэффициентов влияния, что является основным направлением дальнейших исследований.

Литература

1. Ushakov, I.A. *Reliability: past, present, future [Electronic resource]* / I.A. Ushakov // *Reliability: Theory & Applications*. – 2006. – Vol.1, № 1(01). – P. 10 – 16. – Access mode: http://www.gnedenko-forum.org/Journal/2006/012006/art_1_01%281%29_2006.pdf. – 20.12.2012y.

2. Ushakov, I.A. *Reliability theory: history & current state in bibliographies [Electronic resource]* / I.A. Ushakov // *Reliability: Theory & Applications*. – 2012. – Vol.7, № 1(24). – P. 10 – 16. – Access mode: http://www.gnedenko-forum.org/Journal/2012/012012/RTA_1_2012-01.pdf. – 20.12.2012 y.

3. Singpurwalla, N.D. (1995). *The failure rate of software: does it exist?* [Text] / N.D. Singpurwalla, // *IEEE Transactions on Reliability*. – Vol.44, No. 3. – P. 34 – 41.

4. CASE-оценка критических программных систем. Т. 2. Надежность = CASE-Assessment of critical

software systems. Vol. 2. Reliability: [Text] / О.Н. Одарущенко, В.С. Харченко, Д.А. Маевский и др. / Под ред. Харченко В.С. – X.: Нац. аэрокосм. ун-т им. Н.Е. Жуковского «ХАИ», 2012. – 292 с.

5. Maevsky, D.A. *Software reliability. Non-probabilistic approach [Electronic resource]* / D.A. Maevsky, H.D. Maevskaya, A.A. Leonov // *Reliability: Theory & Applications*. – 2012. – Vol. 7, № 3(26). – P. 8 – 20. – Access mode: http://www.gnedenko-forum.org/Journal/2012/032012/RTA_3_2012-01.pdf. – 20.12.2012 y.

6. Maevsky, D.A. *Fundamentals of software stability theory [Electronic resource]* / D. A. Maevsky // *Reliability: Theory & Applications*. – 2012. – Vol.7, № 4(27). – P. 31 – 40. – Access mode: http://www.gnedenko-forum.org/Journal/2012/042012/RTA_4_2012-03.pdf. – 20.12.2012 y.

Поступила в редакцию 28.02.2013, рассмотрена на редколлегии 27.03.2013

Рецензент: д-р техн. наук, проф., зав. каф. компьютерных систем и сетей В.С. Харченко, Национальный аэрокосмический университет им. М.С. Жуковского «ХАИ», Харьков

ОЦІНКА ПОКАЗНИКІВ НАДІЙНОСТІ БАГАТОКОМПОНЕНТНИХ ПРОГРАМНИХ СИСТЕМ

Д.А. Маєвський

У роботі виконано розширення теорії динаміки програмних систем на випадок Web і Cloud- систем, що мають багатокомпонентну структуру. Розглянуто потоки дефектів у багатокомпонентних системах і їх взаємні впливи на основі принципів рівноваги, взаємності і суперпозиції. Отримана математична модель процесу виявлення дефектів багатокомпонентних систем у вигляді автономної системи диференціальних рівнянь. Модель описує взаємодію потоків дефектів і дозволяє спрогнозувати кількість дефектів в системі у будь-який момент часу. Тому створену модель можна розглядати як модель надійності багатокомпонентних програмних систем. На прикладі двокомпонентної системи без урахування вторинних дефектів пояснено раніше відмічене явище внутрішньої рівноваги програмних систем.

Ключові слова: багатокомпонентна система, модель надійності, динаміка програмних систем, програмні дефекти, потоки дефектів.

RELIABILITY EVALUATION ON MULTI-SYSTEM SOFTWARE

D.A. Maevsky

This paper presents the extension of the theory of the software systems dynamics for Web and Cloud-systems with multi-component structure. Consider the flow of defects in multi-component systems and their mutual influence on the principles of balance, reciprocity and superposition. We propose the mathematical model of the process of identifying defects multicomponent systems as an autonomous system of differential equations. The model describes the interaction of flow defects and predicts the number of defects in the system at any given time. Therefore, the model generated can be considered as a model of reliability of multi-component software systems. On the example of the two-component system without secondary defects noted previously is explained the phenomenon of internal equilibrium of software systems.

Keywords: Multi-system reliability model, the dynamics of software systems, software defects, the flow defects.

Маевский Дмитрий Андреевич – канд. техн. наук, доцент, заведующий кафедрой теоретических основ и общей электротехники Одесского национального политехнического университета, Одесса, Украина, e-mail: Dmitry.A.Maevsky@gmail.com.