УДК 62(07)

СТАТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

О.О. Павловская

STATIC METHODS OF ASSESSMENT OF SOFTWARE

O.O. Pavlovskaya

В статье показаны особенности использования математического аппарата прикладной теории надежности технических систем для определения показателей надежности программного обеспечения (ПО). Этот материал необходим студентам, аспирантам, практикам для получения возможности оценки влияния различных внутренних и внешних факторов на качество функционирования ПО.

Ключевые слова: оценка надежности, теория надежности, программное обеспечение.

The article shows the features of the use of mathematical apparatus applied the theory of reliability of technical systems for determining the reliability of software (SW). This material is needed for students, graduate students, practitioners to be able to assess the impact of various internal and external factors on the quality of the software.

Keywords: reliability estimation, reliability theory, software.

Введение

В настоящее время актуальной является проблема исследования надежности программного обеспечения (ПО). В рамках данной проблемы можно выделить ряд частных задач, таких как:

- определение основных факторов, влияющих на надежность ПО;
- разработка методов оценки надежности ПО;
-разработка методов, обеспечивающих достижение заданного уровня надежности ПО.

Под надежностью ПО понимается его способность безотказно выполнять определенные функции при заданных условиях в течение заданного периода времени с достаточно большой вероятностью.

Составляющие функциональной надежности ПО

1. Безотказность - свойство программы выполнять свои функции во время эксплуатации.

2. Работоспособность - свойство программы корректно (как ожидает пользователь) работать весь заданный период эксплуатации.

3. Безопасность - свойство программы быть неопасной для людей и окружающих систем.

4. Защищенность - свойство программы противостоять случайным или умышленным вторжениям в нее.

Факторы, влияющие на надежность ПО, делят на 2 группы.

1. Внутренние (ошибки проектирования при постановке задач; ошибки алгоритмизации задач; ошибки программирования; недостаточное качество средств защиты).

2. Внешние (ошибки персонала при эксплуатации; искажения информации в каналах связи; сбои и отказы аппаратуры ЭВМ).

Процентные частоты появления ошибок в ПО по типам ошибок представлены в таблице [2, с. 103].

Частота появления ошибок в ПО

Тип ошибки	Частота появления, %
Неполная или ошибочная спецификация	28
Отклонение от спецификации	12
Пренебрежение правилами программирования	10
Ошибочная выборка данных	10
Ошибочная логика или последовательность операций	12
Ошибочные арифметические операции	9
Нехватка времени для решения	4
Ошибка обработки прерываний	4
Ошибка в исходных данных	3
Неточная запись	8

Как видно из таблицы, основное количество ошибок делается из-за неверной спецификации и следует обращать особое внимание на проведение тестирования ПО с намерением, во-первых, найти и исправить ошибки в ПО, снижающие надёжность последнего, а во-вторых, определить надежность ПО.

Павловская Ольга Олеговна – канд. техн. наук, доцент каф. «Системы управления» ЮУрГУ; olyapav@rambler.ru

Pavlovskaya Olga Olegovna – PhD, associate professor of Control Systems Department of SUSU; olyapav@rambler.ru

Оценка надежности ПО, как и любого другого объекта, начинается с определения признаков, по которым будет оцениваться надежность объекта (так называемых критериев надежности).

1. Критерии надежности ПО

При анализе надежности ПО используются традиционные для технических систем критерии надежности.

1. Вероятность безотказной работы $P(t_з)$.
2. Вероятность отказа $Q(t_з)$.
3. Интенсивность отказов $\lambda(t)$.
4. Средняя наработка на отказ T_0.
5. Среднее время восстановления $T_в$.
6. Коэффициент готовности $K_г$.

Традиционные критерии надежности ПО характеризуют наличие ошибок программы (производственных дефектов), но ни один из них не характеризует характер этих ошибок и возможные их последствия. Поэтому вводится дополнительный критерий надежности ПО - *средняя тяжесть ошибок* (СТО) [1, с. 122], определяемый выражением

$$\text{СТО} = \frac{1}{Q}\sum_{i=1}^{m} b_i p_i z_i ,$$

где Q - вероятность сбоя ПО; b_1 - функция принадлежности тяжести последствий ошибки, возникшей при i-м наборе входных данных, к максимально тяжелым последствиям; p_i - вероятность ввода i-го набора входных данных при эксплуатации ПО; z_i- дихотомическая переменная, равная 1, если при l-м наборе входных данных был зафиксирован сбой, и 0 в противном случае; m - общее число наборов входных данных.

Значение показателя надежности СТО лежит на интервале [0; 1]. Чем ближе значение СТО к единице, тем тяжелее последствия ошибок ПО, и тем менее надежна программа. Близость СТО к нулю показывает незначительность последствий ошибок программы.

Введение данного критерия надежности ПО позволяет характеризовать не столько безошибочность ПО, сколько его безопасность. Однако следует помнить, что значение этого критерия субъективно и может быть различным для одного и того же программного продукта в зависимости от области его применения. Это объясняется тем, что при использовании конкретного ПО, например для выполнения студенческих расчетов и для выполнения конструкторских расчетов в космической промышленности последствия ошибок программы - несопоставимы. В ряде случаев, если к ПО предъявляются жесткие требования, лучше оценивать максимальную тяжесть ошибок ПО.

Основным средством определения показателей надежности являются *модели надежности,* под которыми понимают математическую модель, построенную для оценки зависимости надежности от заранее известных или оцененных в ходе создания ПО параметров.

2. Модели надежности ПО

Различают модели ПО статические и динамические. Статические модели принципиально отличаются от динамических прежде всего тем, что в них появление отказов не связывают со временем появления ошибок в процессе тестирования, а учитывают только зависимость количества ошибок от числа тестовых прогонов (по области ошибок) или зависимость количества ошибок от характеристики входных данных (по области данных). В динамических же моделях поведение ПО (появление отказов) рассматривается во времени.

Рассмотрим статические модели надежности ПО [3, с. 167].

2.1. Статическая модель надежности Миллса

Использование этой модели предполагает необходимость перед началом тестирования искусственно вносить в программу (засорять) некоторое количество известных ошибок. Ошибки вносятся случайным образом и фиксируются в протоколе искусственных ошибок. Специалист, проводящий тестирование, не знает ни количества ошибок, ни характера внесенных ошибок до момента оценки показателей надежности по модели Миллса. Предполагается, что все ошибки (как естественные, так и искусственно внесенные) имеют равную вероятность быть найденными в процессе тестирования.

Тестируя программу в течение некоторого времени, собирается статистика об ошибках. В момент оценки надежности по протоколу искусственных ошибок все ошибки делятся на собственные и искусственные.

Модель надежности Миллса образуется двумя связанными между собой по смыслу соотношениями.

*Первое соотношN = S·n/V*предсказывает N - первоначальное количество ошибок в программе. В данном соотношении, которое называется формулой Миллса, S - количество искусственно внесенных ошибок, и - число найденных собственных ошибок, V - число обнаруженных к моменту оценки искусственных ошибок.

Предположим, что в программе имеется K собственных ошибок, и внесем в нее еще S ошибок. Если в процессе тестирования были обнаружены все S внесенных ошибок и и собственных ошибок, то по формуле Миллса мы предполагаем, что первоначально в программе было $N = n$ ошибок.

Второе соотношение используется для установления доверительного уровня прогноза C (вероятности, с которой можно высказать предположение об N). Величина C является мерой доверия к модели.

Если обнаружены все искусственно рассеянные ошибки $(V = N)$ вероятность того, что значение N найдено правильно, можно рассчитать по следующему соотношению:

$$C = S/(S + K + 1).$$

В случае, когда оценка надежности производится до момента обнаружения всех S рассеянных ошибок, величина C рассчитывается по модифицируемой формуле

$$C = \left(\frac{S}{V-1}\right) \Big/ \left(\frac{S+K+1}{V+K}\right),$$

где числитель и знаменатель формулы являются биноминальными коэффициентами вида

$$\frac{a}{b} = \frac{a!}{b!(a-b)!}.$$

Например, если утверждается, что в программе нет ошибок, а к моменту оценки надежности обнаруженно 5 из 10 рассеянных ошибок и не обнаружено ни одной собственной ошибки, то вероятность того, что в программе действительно нет ошибок, будет равна

$$C = \left(\frac{10}{4}\right) \Big/ \left(\frac{11}{5}\right) = \frac{10! \cdot 5! \cdot 6!}{4! \cdot 6! \cdot 11!} = 0{,}45.$$

Если при тех же исходных условиях оценка надежности производится в момент, когда обнаружены 8 из 10 искусственных ошибок, то вероятность того, что в программе не было ошибок, увеличивается до 0,73.

В действительности модель Миллса можно использовать для оценки N после каждой найденной ошибки. Предлагается во время всего периода тестирования отмечать на графике число найденных ошибок и текущее значение для N.

Достоинством модели является простота применения математического аппарата, наглядность и возможность использования в процессе тестирования. Однако модель не лишена и ряда недостатков, самые существенные из которых - это необходимость внесения искусственных ошибок (этот процесс плохо формализуется) и достаточно вольное допущение величины K, которое основывается исключительно на интуиции и опыте человека, проводящего оценку, т.е. допускается большое влияние субъективного фактора.

2.2. Статическая модель надежности Липова

Липов модифицировал модель Миллса, сделав то же предположение, что и Миллса, т.е. что собственные и искусственные ошибки имеют равную вероятность быть найденными.

Тогда вероятность обнаружения η собственных и V внесенных ошибок равна

$$Q(n,V) = \frac{m}{n+V} \cdot q^{n+V} \cdot (1-q)^{m-n-\frac{V \cdot \frac{N}{n} \cdot \frac{S}{V}}{\left(\frac{N+S}{n+V}\right)}},$$

где m – количество тестов, используемых при тестировании; q – вероятность обнаружения ошибки в каждом из m тестов, рассчитываемая по формуле $q = (n+V)/n$; S – общее количество искусственно внесенных ошибок; N – количество собственных ошибок, имеющихся в ПС до начала тестирования.

Для использования модели Липова должны выполняться следующие условия: $N \geq n \geq 0$, $S \geq V \geq 0$, $m \geq n+V \geq 0$.

Заключение

1. Особенностью оценки надежности ПО является использование наряду с традиционными критериями надежности, такого специфического критерия, как СТО. Введение данного критерия надежности ПО позволяет характеризовать не только безошибочность ПО, но и его безопасность.

2. Основным средством определения показателей надежности являются модели надежности.

3. Статические модели не связывают появление отказов со временем появления ошибок в процессе тестирования, а учитывают только зависимость количества ошибок от числа тестовых прогонов (по области ошибок) или зависимость количества ошибок от характеристики входных данных (по области данных).

4. Модель Липова дополняет модель Миллса, дав возможность оценить вероятность обнаружения определенного числа ошибок к моменту оценки.

Литература

1. Игнатьев, М.Б. Активные методы обеспечения надежности алгоритмов и программ / М.Б. Игнатьев, В.В. Фильчаков, Л.Г. Осовецкий. - СПб.: Политехника, 1992.

2. Липаев, В. В. Надежность программных средств / В.В. Липаев. -М.: СИНТЕГ, 1998.

3. Половко, А.М. Основы теории надежности / А.М. Половко, СВ. Гуров. - 2-е изд., перераб. и доп.-СПб.: БХВ-Петербург, 2006.

Поступила в редакцию 2 октября 2007 г.