УДК 519.8

А. В. Титов

МЕТОДИКА ОЦЕНКИ НАДЕЖНОСТИ ВСТРОЕННЫХ ПРОГРАММНЫХ СРЕДСТВ ПРИ РЕДКИХ ОТКАЗАХ

Рассматривается задача анализа надежности программного обеспечения систем стратегического назначения и методы оценки параметров надежности по малому числу наблюдений. Предложен метод объединения данных, полученных для различных технических объектов со встраиваемыми программными средствами.

Ключевые слова: *надежность программных средств, редкие отказы*.

Анализ надежности встроенных программных средств — сложная комплексная задача, требующая использования аппарата теории вероятностей и математической статистики. В системах ответственного назначения отказы являются редкими событиями [1]. Ограниченного объема данных бывает недостаточно для того, чтобы найти заранее неизвестный закон распределения времени между программными сбоями. Тем не менее, если вид закона распределения известен, то его параметры могут быть оценены по имеющейся информации.

В настоящей работе рассматривается система передачи данных, функционирующая на нескольких однотипных технических объектах одновременно. В качестве наблюдаемых характеристик системы выбраны время наработки на отказ и время восстановления после отказа. Под отказом понимается сбой в работе программных средств, требующий восстановления их работоспособности [1].

Исследование особенностей функционирования рассматриваемой системы, а также сбор статистических данных значительно упрощаются, если объединять данные наблюдений, полученные для различных технических объектов. При таком объединении возможно появление ошибок, связанных, во-первых, с различиями в организации эксплуатации технических объектов, например, с недостаточным уровнем подготовки операторов и, во-вторых, с ненадлежащим сопровождением программных средств [2]. Каждое программное средство может подразделяться на модули, каждый из которых может рассматриваться как самостоятельный объект исследования.

В качестве основных характеристик надежности рассматриваются время наработки на отказ и время восстановления после отказа. Отказы программного средства фиксируются в журнале, где указывается время отказа, время восстановления и модуль, в котором был зарегистрирован отказ.

Если условия функционирования объектов могут различаться и влиять на интенсивность появления программный сбоев, то возникает проблема построения решающего правила, по которому возможно объединение результатов наблюдений, т.е. возникает задача выбора максимального количества данных наблюдений, соответствующих однотипным внешним условиям. Факт неоднородности результатов наблюдений может быть установлен на основе дисперсионного анализа [3]. В некоторых случаях возможно построение нескольких пересекающихся или непересекающихся серий наблюдений.

Неправильно полагать, что система останавливается в момент любого отказа. Следует учитывать, что рассматриваемые объекты изолированы. Объединяя данные, необходимо знать, не является ли расхождение в средних значениях времени наработки на отказ и времени восстановления случайным, либо проявляется влияние периодически возникающих факторов [3]. Если такие факторы выявлены, то их влияние можно скорректировать, непосредственно изменяя элементы выборки.

Предлагается проверять возможность объединения по следующей схеме:

1) проверяются данные наблюдений для всех однотипных программных модулей; если для модуля ни разу не фиксировались отказы, то модуль исключается из рассмотрения;

2) для всех модулей, где возможен расчет среднего времени наработки на отказ, проводятся необходимые вычисления, формируются средние значения времени между отказами для каждого модуля;

3) полученные средние значения времени наработки на отказ сортируются по убыванию;

4) в полученном списке определяется статистическая значимость расхождений между данными модулями;

5) если статистическая значимость расхождения ниже заданного уровня, то осуществляется попарное объединение смежных серий наблюдений, в противном случае объединение не производится;

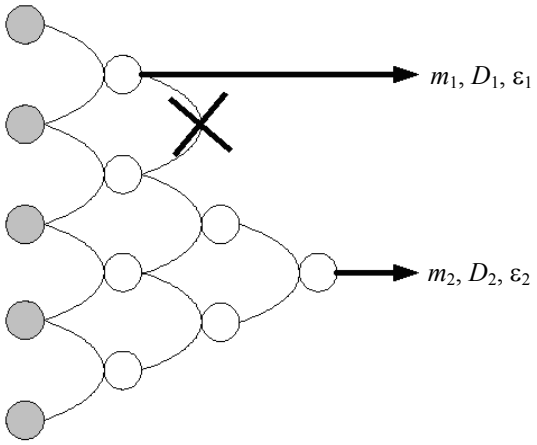
6) проводится расчет среднего времени наработки на отказ в объединенных выборках;

7) шаги 5—7 повторяются, пока не произойдет максимально возможное объединение, при этом возможны несколько ветвей объединения;

8) для полученных объединенных выборок вычисляются необходимые параметры: оценки математического ожидания, дисперсии и величины доверительного интервала для математического ожидания (m, D, ε).

Приведенная последовательность действий иллюстрируется рисунком (серыми кружками обозначены данные наблюдений для каждого из модулей; белые кружки соответствуют объединенным сериям наблюдений; дуги между кружками означают, что значимость различий меньше заданного уровня и объединение возможно; невозможное объединение

перечеркнуто). После всех итераций имеются два результата объединения, каждый со своими параметрами.



Представленный метод проиллюстрирован примером. Даны результаты работы четырех однотипных модулей (l) и средние значения их времени наработки на отказ $t_{\text{ср}}^{i}$ в условных единицах времени (табл. 1). Определены средние значения времени наработки на отказ для каждой серии наблюдений. В табл. 2 средние значения отсортированы по убыванию.

Таблица 1

Результаты работы однотипных модулей системы

№ серии			
1	2	3	4
10,508	10,135	10,775	10,662
10,184	10,006	10,717	10,447
9,876	9,853	10,579	10,696
10,116	9,906	10,563	10,925
10,199	9,954	10,285	10,386
10,385	10,633	10,122	10,357
10,678	10,511	10,958	10,170
10,006	10,270	10,715	10,160
10,132	10,218	10,992	10,039
10,814	9,969	10,634	10,324
$t_{\text{ср}}^{(1)}$=10,290	$t_{\text{ср}}^{(2)}$=10,145	$t_{\text{ср}}^{(3)}$=10,634	$t_{\text{ср}}^{(4)}$=10,417

Таблица 2

„Соседние“ значения среднего времени наработки на отказ

№ серии	$m^{(i)} = t_{\text{ср}}^{(i)}$
3	10,634
4	10,417
1	10,290
2	10,145

После сортировки проверяется значимость расхождения между смежными средними значениями. Используются стандартные тесты для несвязанных серий наблюдений [3]. Результатом является определение статистической значимости.

Проанализировав полученные объединенные наборы, содержащие в себе данные четвертого и первого, первого и второго модулей соответственно, получим следующие результаты. Средние значения каждой новой серии равны:

$$t_{\text{ср}}^{(4-1)} = m_2 = 10{,}353,$$
$$t_{\text{ср}}^{(1-2)} = m_3 = 10{,}218.$$

Разность между средними равна: $\Delta m = 0{,}136$; среднее по обеим сериям: $m = 10{,}285$; дисперсия $D = 0{,}082\,129$, откуда $\sigma = 0{,}090\,625$.

Вероятность значимости расхождения: $P = 0{,}066\,81$, поскольку вероятность выше принятого уровня значимости, расхождения между сериями случайны.

Таким образом, были получены два варианта объединения наблюдений: первая содержит данные о работе третьего модуля, вторая — объединенные данные, полученные для четвертого, первого и второго модулей.

Объединенная серия наблюдений существенно сузит границы значений показателей надежности. Например, при заданном уровне достоверности 95 % доверительный интервал для времени наработки на отказ модуля номер три определяется как $10{,}634 \pm \Delta t_{\text{ср}}^{(4)} = 0{,}14$. Границы доверительного интервала для объединенной серии наблюдений существенно у́же: $10{,}284 \pm \Delta t_{\text{ср}}^{(4-1-2)} = 0{,}07$.

Для увеличения объема статистической базы исследования целесообразно объединять результаты наблюдений для встраиваемых программных средств. Если условия функционирования объектов могут различаться и влиять на характеристики серий наблюдений, то возникает проблема построения решающего правила, по которому возможно объединение серий, т.е. при объединении серий наблюдений возникает задача построения максимальной по объему серии, такой, что между входящими в ее состав исходными сериями отсутствуют статистически значимые различия. Факт неоднородности наблюдений может быть установлен на основе дисперсионного анализа. В некоторых случаях возможно построение нескольких пересекающихся или непересекающихся объединенных серий наблюдений.

Предложенная методика объединения статистических данных может быть использована при анализе отказов программных средств однотипных изолированных отказоустойчивых систем.

СПИСОК ЛИТЕРАТУРЫ

1. *Майерс Г.* Надежность программного обеспечения. М.: Мир, 1980. 360 с.

2. *Шафер Д. Ф., Фатрелл Р. Т., Шафер Л. И.* Управление программными проектами: достижение оптимального качества при минимуме затрат. М.: Вильямс, 2003. 1136 с.

3. *Вентцель Е. С., Овчаров Л. А.* Теория вероятностей и ее инженерные приложения. М.: Наука, 1988. 480 с.

Сведения об авторе

Алексей Владимирович Титов — аспирант; Национальный исследовательский ядерный университет, кафедра № 12 компьютерных систем и технологий, Москва;
E-mail: m-p-r@inbox.ru

Рекомендована кафедрой
компьютерных систем и технологий

Поступила в редакцию
15.03.10 г.