остаются радиоактивными не более 100 лет, что значительно меньше по сравнению с хранением ОЯТ, сохраняющего высокую активность сотни лет.

Недостатки МОХ-топлива: не до конца отработанная технология изготовления МОХ-топлива из ОЯТ, накопленного после работы в тепловых реакторах, в связи с чем изготовление данного вида топлива приблизительно в 3 раза дороже обычного топлива; данный вид топлива имеет более нестабильное состояние, а также более жесткие требования к режимам эксплуатации.

Ближайшая перспектива развития БАЭС заключается в совершенствовании и оптимизации проекта БН-800, использовании в его активной зоне только смешанного уран-плутониевого МОХ-топлива [8].

***

1. Nuclear Share of Electricity Generation in 2017 [Электронный ресурс] // International Atomic Energy Agency URL: <https://pris.iaea.org/PRIS/WorldStatistics/NuclearShareofElectricityGeneration.aspx>
2. Operational & Long-Term Shutdown Reactors [Электронный ресурс] // International Atomic Energy Agency URL: <https://pris.iaea.org/PRIS/WorldStatistics/OperationalReactorsByCountry.aspx>
3. Атомная энергетика: аргументы «за» и «против» [Электронный ресурс] // Экорепортер URL: <http://ecoreporter.ru/node/336>
4. Генерация электроэнергии [Электронный ресурс] // Росатом URL: <https://www.rosatom.ru/production/generation/>
5. Атомная энергетика и ее безопасность [Электронный ресурс] // Кафедра молекулярной физики ФТФ, УГТУ-УПИ URL: <http://molphys.ustu.ru/Study/Atom/cap4.html>
6. Переработку отработавшего ядерного топлива с Белоярской АЭС начнут в 2024 году [Электронный ресурс] // ТАСС URL: <https://tass.ru/ural-news/6090214>
7. МОКС топливо, MOX топливо (англ. Mixed-Oxide fuel) [Электронный ресурс] // Neftegaz.ru URL: <https://neftegaz.ru/tech-library/energoresursy-toplivo/142131-moks-toplivo-mox-toplivo-angl-mixed-oxide-fuel/>
8. Блок Белоярской АЭС БН-800: новые перспективы атомной энергетике [Электронный ресурс] // Атомная энергия URL: <http://www.atomic-energy.ru/interviews/2015/12/18/62072>

Ермошкин В.И., Фенюк Е.Е., Щербинко А.В.

Квалиметрическая оценка надёжности программного обеспечения сложных радиоэлектронных систем

*ЗАО НИЦ «РЕЗОНАНС»
(Россия, Москва)*

doi: 10.18411/sr-10-08-2019-07

idsp: sciencerrussia-10-08-2019-07

Аннотация

При разработке новых сложных радиоэлектронных систем (РЭС) для подтверждения тактико-технических характеристик силами предприятий разработчиков и изготовителей проводятся различные виды испытаний.

Ключевые слова: радиоэлектронные системы, программное обеспечение, квалиметрическая оценка, средства вычислительной техники.

Наиболее сложные, дорогостоящие, трудоемкие и длительные виды испытаний - испытания на надежность которые составляют 70% всех затрат на испытания. Следовательно, экспериментальное определение параметров надежности изделия, в том числе и программного обеспечения (ПО), обеспечивающего функционирование РЭС, к которым относятся безотказность, долговечность, сохраняемость и ремонтпригодность являются актуальной задачей. Расчетные оценки могут быть завышенными.

Для квалиметрической оценки показателей надежности на соответствие заданным, испытания РЭС проводят с большой интенсивностью.

Этот вид испытаний можно считать разрушающим, поскольку испытываемые РЭС расходуют значительную часть своего ресурса. Серийные образцы сложных РЭС являются дорогостоящими устройствами, и данные испытания могут быть экономически не выгодными.

С целью сокращения времени и ресурсов при испытании ПО на надежность применяются ускоренные испытания, позволяющие дать оценку показателей надежности ПО за время, более короткое, чем при нормальных условиях эксплуатации.

Методики ускоренных испытаний на надежность сложных РЭС приведены в различных нормативных документах [6, 7, 8].

Для получения квалитетической оценки в ходе ускоренных испытаний предлагается следующий методический аппарат. При обработке результатов ускоренных испытаний необходимо знать закономерности поведения систем при воздействии на них тех или иных факторов и режимов. Если эти закономерности известны, то всегда можно выбрать такой режим, при котором испытания будут продолжаться очень короткое время.

В статье [1] предложен принцип получения данных о надежности функционирования программного обеспечения (ПО) на основе форсирования быстрогодействия ЭВМ. Для оценки надёжности ПО АСУ сложных РЭС ускорение испытаний также возможно на средствах вычислительной техники (СВТ), работающих в реальном масштабе времени, за счёт увеличения интенсивности загрузки вычислительными задачами: ускорения потока входных данных, эмуляции действий оператора АСУ и прочих. Полученные данные представляются в виде плотности или функции распределения времени до ошибок, возникающих в процессе выполнения программы. Затем эти распределения пересчитываются в соответствующие распределения при нормальных (штатных) условиях выполнения программы. Пересчет от одних условий к другим может быть выполнен только в том случае, когда известна зависимость интенсивности возникновения ошибки (или другой связанной с ней характеристики) от параметра форсирования. В качестве параметра форсирования выбрана интенсивность загрузки задачами СВТ [3] относительно значений при штатном функционировании ПО.

Предположим, что длительность тестирования некоторого ПО на штатном СВТ с интенсивностью задач B_0 равна t_0 единиц времени. Вероятность ошибки на одну команду в СВТ с интенсивностью B положим равной:

$$\square(B) = \square_0 + \square(B - B_0)^m, \quad (1)$$

где $\square_0$ – вероятность ошибки на одну команду в СВТ с интенсивностью B_0 ,

$\square$ – коэффициент пропорциональности вероятности ошибки загрузке задачами СВТ, m – степенной коэффициент. B – есть загрузка технологического (испытательного) СВТ. Найдём, каким должно быть время тестирования ПО $\square_T$ на технологическом СВТ с интенсивностью $B > B_0$, чтобы вероятность отсутствия ошибки на штатном СВТ за время $\square_0$ была бы равна вероятности отсутствия ошибки на технологическом СВТ.

Считая вероятность ошибки на одну команду малой величиной, запишем выражение для вероятности отсутствия ошибки ПО за время испытаний на технологическом СВТ [4]:

$$P(\tau_T) = (1 - \beta)^{\tau_T B} \approx \exp\left[-\left[\beta_0 + \alpha(B - B_0)^m\right] \cdot B \cdot \tau_T\right]. \quad (2)$$

Вероятность отсутствия ошибки на штатном СВТ за время испытаний $\square_0$ будет равна:

$$P(\tau_0) = (1 - \beta_0)^{\tau_0 B_0} \approx e^{-\beta_0 B_0 \tau_0}. \quad (3)$$

Приравнявая (2) и (3), находим:

$$\tau_T = \frac{\tau_0}{\left[1 + \frac{\alpha B_0^m}{\beta_0} (K_B - 1)^m \right] K_B}, \quad (4)$$

где $K = B/B_0$ – коэффициент форсирования нагрузки на СВТ.

Для реализации описанной методики испытательный стенд должен содержать следующие основные компоненты. Прежде всего его элементом является технологическая ЭВМ. Данная ЭВМ должна иметь запас вычислительной мощности достаточный для выполнения задач АСУ РЭС с заданным коэффициентом форсирования. Интенсивность загрузки задачами СВТ может быть задана до начала испытаний или динамически изменяться оператором или специализированным ПО в ходе выполнения тестов в зависимости от использования ресурсов технологической ЭВМ в данный момент. Практически легче реализовать дискретное изменение интенсивности загрузки с помощью встроенного переключателя.

Загрузка технологической ЭВМ должна производиться типовыми входными данными, характерными для штатной работы, рассматриваемой РЭС, а также эмуляцией действий оператора [9], в том числе заведомо ошибочных, автоматически последовательно - после завершения обработки предшествующих наборов данных или фиксации прерываний АСУ из-за обнаруженных ошибок. Этот процесс следует осуществлять с помощью управляющей ЭВМ, снабжённой соответствующим программным управлением.

Третьим элементом стенда является программный или аппаратно–программный контроль состояния функционирующей программы. При этом нужно осуществлять контроль окончания выполнения программы и правильности полученного результата или контроль процесса срыва нормального её функционирования.

Четвёртый элемент стенда служит для накопления числа выполненных на ЭВМ прогонов и числа срывов программ. Им же осуществляется и математическая обработка полученных статистических данных о надёжности ПО в результате форсированных испытаний.

***

1. Смагин В.А., Солдатенко В.С., Кузнецов В.В. Моделирование и обеспечение надёжности программных средств АСУ. – СПб.: ВИКУ им. А.Ф. Можайского. – 1999. – 49 с.
2. В.В. Липаев. Надёжность и функциональная безопасность комплексов программ реального времени. – М.: Институт системного программирования РАН, 2013.
3. Липаев В.В. Надёжность программных средств. – М.: СИНТЕГ, 1998. – 232 с.
4. Смагин В.А. Техническая синергетика. Вып.1. Вероятностные модели элементов сложных систем. – СПб.: ВИКУ им. А.Ф. Можайского, 2000. – 63 с.
5. Надёжность в технике. Методы контроля показателей надёжности и планы контрольных испытаний на надёжность ГОСТ 27.410—87. – 79с.
6. Руководящий нормативный документ. Методические указания. Надёжность в технике. Ускоренные испытания. Основные положения РД 50-424-83; СГИП. - 12с.
7. Руководящий нормативный документ. Комплексная система контроля качества. Аппаратура, приборы, устройства и оборудование военного назначения. Типовые методики ускоренных испытаний на безотказность и долговечность РД В 319.01.11-98, изд. Минобороны РФ, Технический комитет по военной стандартизации №319 «Надёжность и стойкость ЭРИ и РЭА военного назначения», 2000. – 91с.
8. Федоров В.К., Сергеев Н.П., Кондрашин А.А. Контроль и испытания в проектировании и производстве радиоэлектронных средств. – М.: Техносфера, 2005. – 504с.
9. ISO/IEC/IEEE 29119-1:2013 Software and systems engineering — Software testing Part 1: Concepts and definitions(ГОСТ Р 56920 - 2016) – 28с - 29с.