ХАРАКТЕРИСТИКИ НАДЕЖНОСТИ РАСПРЕДЕЛЕННЫХ КРИПТОГРАФИЧЕСКИХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ С ОГРАНИЧЕННЫМИ РЕСУРСАМИ*

Р. В. Мещеряков, А. А. Шелупанов
Томский государственный университет систем управления и радиоэлектроники, Россия
e-mail: mrv@security.tomsk.ru

Т. Ю. Зырянова
Уральский государственный университет путей сообщения Екатеринбург, Россия

Reliability criteria for information-telecommunicational systems are considered. Special attention is given to the systems with limited resources. In particular, we consider the problems of quality assurance for such systems and the ways to improve the quality.

1. Основные эксплуатационные характеристики системы передачи данных

На надежность функционирования распределенных криптографических информационно-телекоммуникационных систем с ограниченными ресурсами (РКИТКСОР) влияет множество факторов. Рассмотрим эти факторы подробнее [1–4].

Качество вычислительной системы — это совокупность свойств данной продукции (аппаратуры и программного обеспечения), обусловливающих ее способность удовлетворять определенные потребности в соответствии с назначением системы.

Общая полезность РКИТКСОР может характеризоваться:

— исходной полезностью, к которой можно отнести надежность, эффективность, учет человеческого фактора;

— удобством эксплуатации (оцениваемость, понятность, модифицируемость, мобильность).

*Работа выполнена при финансовой поддержке СО РАН (код проекта 1.10 “Разработка методов и средств создания распределенных информационно-телекоммуникационных систем” согласно постановлению Президиума СО РАН № 54 от 09.02.2006).

Введем базовые понятия.

Работоспособность — состояние РКИТКСОР, при котором он выполняет заданную функции с параметрами, установленными в техническом задании.

Надежность — свойство РКИТКСОР сохранять работоспособность в течение определенного периода времени и в определенных условиях эксплуатации с учетом последствий для пользователей каждого отказа.

Понятность (ясность) — комплексная характеристика, в которую входят:

— информативность (РКИТКСОР снабжен справочно-информационной службой и документацией);

— открытость РКИТКСОР (функционально допустимая расширяемость);

— согласованность — единое требование к оформлению всех аппаратных модулей и блоков программ;

— структурируемость;

— мобильность — возможность внесения изменений без значительных затрат на отладку;

— максимальная независимость от типа ЭВМ и операционной системы.

Очевидно, что прежде всего важны эксплуатационные характеристики: производительность П, коэффициент эффективности $K_э$, коэффициент готовности $K_г$, коэффициент использования $K_и$, надежность, работоспособность.

Несмотря на наличие множества систем передачи данных, наличие ошибок в нем неизбежно. Комплексной характеристикой качества программного обеспечения (ПО) РКИТКСОР может служить плотность оставшихся дефектов после поставки его заказчику. В свою очередь, под плотностью дефектов или ошибок принимают определенное отношение количества дефектов ПО к общему резерву в программном коде. При оценке количества дефектов считается, что дефект может содержаться в любой строке программного кода, но тогда можно полагать, что распределение плотности вероятностей строк кода, содержащих дефекты, подчиняется нормальному закону распределения (закону Гаусса).

На **производительность** вычислительной системы оказывает влияние не только производительность процессора, но и скорость выполнения операций другими функциональными блоками (время цикла обращения к памяти, тактовая частота работы системной шины и т. п.).

В нашем случае производительность программного обеспечения РКИТКСОР оценивается по скорости выполнения некоторого априори заданного ансамбля команд (имеются соответствующие стандарты):

$$П = \frac{\Sigma K_S}{\Sigma K_S T_s} \quad \text{при } S = 1, \ldots, n,$$

где K_S — весовой коэффициент S-й команды; T_S — продолжительность выполнения этой команды. Но эта характеристика справедлива лишь для исправно работающей ЭВМ.

Эффективность — выполнение требуемых функций при минимальных затратах ресурсов. Определить коэффициент эффективности $K_э$ можно по формуле

$$K_э = \frac{П}{C_{ЭВМ} + C_{экс}}$$

или

$$K_э = \frac{П}{C_{ЭВМ}}, \tag{1}$$

где $C_{ЭВМ}$ — стоимость ЭВМ и программного обеспечения; $C_{экс}$ — расходы на эксплуатацию ЭВМ, т. е. коэффициент эффективности $K_э$ есть отношение производительности к затратам.

При эксплуатации системы РКИТКСОР предположим, что случайным образом во времени происходят **отказы**, т. е. система РКИТКСОР прекращает выполнять функции, определенные **техническим заданием** (ТЗ) или **техническими условиями** (ТУ). Полезное время работы системы составит $T_о$, а общее время

$$T = T_о + T_в + T_{ож}, \tag{2}$$

где $T_в$ — время восстановления работоспособности системы; $T_{ож}$ — время ожидания начала восстановления. Время восстановления $T_в$, в свою очередь, зависит от времени поиска неисправности $t_п$ и времени ее устранения $t_у$:

$$T_в = t_п + t_у.$$

Тогда качество работы системы РКИТКСОР можно характеризовать **коэффициентом готовности**:

$$K_Г = \frac{T_о}{T_о + T_в + T_{ож}}. \tag{3}$$

Из (3) следует, что необходимо не только приглашать квалифицированных специалистов для наладки, поиска причины неисправности системы РКИТКСОР, но и правильно организовать службу поддержки с целью уменьшения времени ожидания по приведению ее в работоспособное состояние.

При длительной эксплуатации системы РКИТКСОР имеет смысл ввести такую оценку, как **среднее время наработки на отказ**:

$$\overline{T_о} = \frac{1}{n}\sum_I T_I, \tag{4}$$

где n — количество интервалов времени T исправного функционирования системы РКИТКСОР.

Для увеличения $\overline{T_о}$ необходимо периодически проводить контрольные испытания системы РКИТКСОР и профилактику в соответствии с регламентом обслуживания. На K контрольных операций будет затрачено время

$$\overline{T_k} = \sum_j T_j.$$

На m профилактических мероприятий будет затрачено время

$$\overline{T_p} = \sum_l T_l.$$

Для оценки совокупного качества работы системы РКИТКСОР введем коэффициент использования

$$K_и = \frac{\Sigma_i T_j - T_k - T_{проф}}{\Sigma_i T_j + \Sigma_i \left(T_{iр} + T_{iвос}\right)}, \tag{5}$$

где i — число отказов; T_j — интервал времени между $(i-1)$-м и i-м нарушениями нормального функционирования РКИТКСОР; T_k — суммарное время работы системы РКИТКСОР, потраченное на контроль **достоверности**; $T_{\text{проф}}$ — время, затраченное на профилактику; $T_{i\text{р}}$ — время ожидания начала ремонта; $T_{i\text{вос}}$ — время восстановления. Упрощенный вариант расчета:

$$K_{\text{и}} = \frac{T_{\text{о}}}{T_{\text{вос}} + T_{\text{о}} + T_{\text{проф}}},$$

где $T_{\text{о}}$ — общее полезное время работы системы. Тогда коэффициент готовности

$$K_{\text{г}} = \frac{T_{\text{о}}}{T_{\text{вос}} + T_{\text{о}}}. \tag{6}$$

Для оценки качества работы системы РКИТКСОР можно использовать различные критерии, в том числе и связанные с ее надежностью.

Критерии надежности [5] представляют собой показатели, позволяющие оценить предпочтительность тех или иных решений по степени достижения основных целей с учетом затрат, при которых эти цели достигаются, что весьма критично для моделируемой нами системы РКИТКСОР, в частности для криптографического контроллера “ВИП”.

Требуется не только установить работоспособность системы, но и количественно оценить соответствие реальных характеристик требованиям технической документации. Из опыта эксплуатации больших систем (более 1000 элементов) известно, что иногда удается связать требования надежности со стоимостными показателями. В случае эксплуатации распределенной системы в качестве критериев используются вероятностные оценки, такие как время безотказной работы, время наработки на отказ, вероятность отказа, интенсивность потока отказов, коэффициент готовности и т. п. Считаем, что это более формализованный подход, позволяющий учесть требование известного критерия minmax.

2. Проблемы при оценке надежности РКИТКСОР

При анализе РКИТКСОР с целью выяснения надежности их работы следует учитывать большую сложность логической организации системы и процессов функционирования, большое число и разнообразие элементов, входящих в ее состав, сложность аппаратно-программного взаимодействия ее частей и большой объем технической документации. Основные особенности РКИТКСОР:

— имеет сложное описание и большой объем технической документации;

— представляет собой совокупность не только аппаратных, но и программных средств, имеющих различные свойства в смысле надежности;

— это совокупность элементов для обработки информации, что требует ведения контроля не только за правильностью ее работы, но за достоверностью обработки информации;

— это объект, работающий при наличии внешних возмущающих факторов (аппаратных, в канале передачи, в канале ввода информации), а также нарушений, связанных с невыполнением регламентных требований.

Для повышения степени надежности используются:

— аппаратно-программные средства автоматизации контроля и диагностики;

— средства автоматического восстановления вычислительного процесса при сбоях;

— автоматизация профилактических испытаний;

— автоматизация накопления и обработки информации о нарушениях нормального рабочего процесса;

— дистанционные средства контроля и диагностики системы РКИТКСОР.

Среди средств обработки информации большое значение имеют сложные территориально разобщенные системы РКИТКСОР, базирующиеся на тесном взаимодействии программно-аппаратных элементов системы РКИТКСОР, а также систем и средств передачи информации.

Работоспособность систем РКИТКСОР в первую очередь зависит от достоверности ввода, хранения и передачи информации по протяженным каналам.

Для повышения помехозащищенности используются специальные методы построения аппаратуры, специальные алгоритмы преобразования передаваемой информации и общесистемные средства повышения надежности работы при наличии помех.

Для повышения помехозащищенности распределенной РКИТКСОР имеет важное значение введение понятия **избыточности**.

Избыточность может быть структурной, информационной, технологической, временной и т. п. [5]. Она позволяет обнаружить и исправить в ряде случаев ошибки, возникающие при работе системы и ее элементов [6].

Структурная избыточность увеличивает количество элементов системы, например, путем введения резервных блоков, параллельных вычислений одной задачи и т. п.

Информационная избыточность обеспечивает систему дополнительной информацией (как, например, о наличии и типе помех) или пояснениями об особенностях эксплуатации системы в конкретных условиях. Это может быть дополнительная информация к решению задачи (например, студенческие шпаргалки повышают надежность получения положительной оценки на экзамене).

Технологическая избыточность программного обеспечения приводит к увеличению его объема и связана с использованием языков высокого уровня, систем отладки и инструментальных средств комплексирования программных модулей.

Алгоритмическая же избыточность должна определяться системными аналитиками на этапе проектирования и может существенным образом влиять на качество работы ПО системы РКИТКСОР.

Таким образом, учитывая, что ресурсы на использование избыточности всегда ограничены, необходимо рациональное распределение их между различными видами избыточности. Повышения надежности работы РКИТКСОР можно достичь с помощью комплекса мероприятий, таких как: повышение надежности программно-аппаратных составляющих, уменьшение распределенности, увеличение ресурсов. Поэтому предложенное методическое и математическое обеспечение позволяет решить проблему повышения надежности работы РКИТКСОР.

Список литературы

[1] Интеллектуальные системы в управлении, конструировании и образовании / Под ред. А.А. Шелупанова. Вып. 2. Томск: STT, 2002. 232 с.

[2] Интеллектуальные системы в управлении, конструировании и образовании / Под ред. А.А. Шелупанова. Вып. 3. Томск: STT, 2004. 216 с.

[3] Интеллектуальные системы в управлении, конструировании и образовании / Под ред. А.А. Шелупанова. Вып. 4. Томск: Изд-во Ин-та оптики атмосферы СО РАН, 2004. 250 с.

[4] Мещеряков Р.В., Шелупанов А.А. Специальные вопросы информационной безопасности. Томск: Изд-во Ин-та оптики атмосферы СО РАН, 2002. 350 с.

[5] Липаев В.В. Надежность программного обеспечения АСУ. М.: Энергоиздат, 1981. 240 с.

[6] Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. / Под ред. Р.Л. Добрушинаи, С.И. Самойленко. М.: Мир, 1976. 594 с.

Поступила в редакцию 23 августа 2007 г.