УДК 621.321

Ю.Л. ПОНОЧОВНЫЙ

Полтавский военный институт связи, Украина

МЕТОД ОБЕСПЕЧЕНИЯ ЗАДАННЫХ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

В статье на основе анализа существующих методов обеспечения надежности информационно-управляющих систем предложено усовершенствовать метод обеспечения заданных показателей надежности распределенных информационно-управляющих систем за счет выбора параметров обновлений программных средств системы.

распределенные информационно-управляющие системы, метод обеспечения надежности, вид неисправностей, обновление программных средств

Введение

Повышение требований к качеству информационно-управляющих систем (ИУС), применяемых в электронной коммерции, Web-серверах, телекоммуникационных сетях и др., обуславливает функционирование их в режиме постоянной готовности, т.е. 24 часа в сутки и 7 дней в неделю. Для надежного функционирования такие ИУС строятся по типовому распределенному принципу с функциональной автономностью территориально разнесенных элементов. Например, ИУС высоконадежных Web-серверов могут строиться на основе кластерных структур.

К надежности ИУС выдвигаются требования (табл. 1), условно представленные в виде так называемых «уровней готовности» (High Availability Level, HAL). В частности к информационно-управляющим системам постоянной готовности выдвигаются требования уровней HAL-4 и HAL-5 [1].

Для обеспечения повышенных требований к надежности ИУС необходимо учитывать все возможные факторы, которые увеличивают длительность простоя системы, и противодействовать им. Как известно, простой системы может быть обусловлен либо восстановлением системы после отказа, вызванного некоторым видом неисправностей, либо проведением мероприятий технического обслуживания (ТО), направленных на предотвращение различных неисправностей системы. Очевидно, что эти составляющие простоя ИУС взаимосвязаны, и уменьшение одной из них приведет к увеличению другой. Поэтому, для минимизации простоев в процессе обеспечения надежности ИУС необходимо моделировать их функционирование с учетом процессов восстановления и обслуживания.

Анализ литературных источников [1, 2] позволяет выделить две группы методов обеспечения надежности ИУС:

– методы повышения безотказности ИУС, обеспечивающие предотвращение, предсказание и устранение явных или скрытых причин отказов системы (fault prevention, fault removal, fault forecasting Means);

– методы построения отказоустойчивых систем, в которых допустимы отказы отдельных составляющих элементов системы (fault tolerance System).

Отказы ИУС принято рассматривать как проявление некоторого множества различных видов неисправностей аппаратной и программной компонент ИУС [1 – 3]. Соответственно, далее рассматриваются методы обеспечения надежности аппаратных средств (АС) ИУС и методы обеспечения надежности программных средств (ПС) ИУС.

Таблица 1

Требования к надежности ИУС

HAL	Уровень готовности (%)	$T_{простоев}$ 1/год	Характеристика системы
1	90,0%	36 дней 12 часов	Необслуживаемая, неуправляемая (unmanaged)
2	99,0%	87 часов 36 минут	Обслуживаемая, управляемая (managed)
3	99,9%	8 часов 46 минут	Хорошо обслуживаемая, хорошо управляемая (well-managed)
4	99,99%	52 минут 33 секунд	Устойчивая к отказам (fault-tolerant)
5	99,999%	5 минут 15 секунд	С высокой готовностью (high-availability)
6	99,9999%	51,5 секунд	С очень высокой готовностью (very-high-availability)
7	99,99999%	5,15 секунд	С ультравысокой готовностью (ultra-availability)

Методы повышения безотказности аппаратной компоненты ИУС предусматривают использование высоконадежных элементов АС на этапе проектирования [3 – 5] и своевременное обнаружение и устранение дефектов АС в процессе ТО на этапе эксплуатации ИУС [4]. Для современных электронных компонентов ИУС порядок интенсивности безотказной работы составляет $10^{-9} – 10^{-6}$ отказов/час [5], поэтому при измерении значений указанного параметра используют относительные величины: FR (failure rate) = 10^{-6} и FIT (failure in time) = 10^{-9}. Методы повышения безотказности программной компоненты ИУС предусматривают проведение качественного тестирования и верификации программных продуктов до ввода их в эксплуатацию [5], а также модернизацию [6] и обновления ПС [7] для устранения дефектов старения и невыявленных дефектов при эксплуатации ПС ИУС. Однако, несмотря на принимаемые меры, среднестатистический уровень невыявленных дефектов составляет 6 единиц на 1000 строк программного кода [5]. Тогда, если быстродействие выполнения программы процессором ИУС составляет $7 \cdot 10^9$ строк кода/час, интенсивность отказов ПС, вызванных дефектами проектирования, составит $2{,}5 \cdot 10^{-3}$ отказов/час [5].

Очевидно, что на данный момент безотказность АС ИУС на несколько порядков выше безотказности ПС ИУС.

Методы повышения отказоустойчивости как АС так и ПС ИУС предусматривают внесение избыточности в физическую или логическую структуру системы. Так отказоустойчивость АС обеспечивается за счет применения резервированных структур (дублированных, троированных, мажоритарно-резервированных и т.д.) [1, 3, 8], а отказоустойчивость ПС обеспечивается их диверсификацией, то есть одновременным использованием программных продуктов различных разработчиков [9]. Применение распределенной структуры ИУС (например, кластерной) позволяет одновременно повысить отказоустойчивость к дефектам АС и к так называемым «heisenbug»-дефектам ПС [6].

Формулирование проблемы. На современном этапе характерно построение ИУС из готовых компонент – вычислительной техники и программного обеспечения универсального назначения, поэтому для обеспечения надежности таких систем, как правило, применяются методы повышения отказоустойчивости. Так в [3, 8] для обеспечения заданных показателей надежности предлагается методика со-

ставления вариативного ряда, из которого выбирается требуемая структура системы.

Однако данная методика может оказаться невостребованной для разработчиков ИУС в силу того, что дополнительное резервирование АС может не потребоваться, так как безотказность современных АС ИУС достаточно высока; а диверсификация ПС неприемлема в силу дороговизны программной продукции. В связи с этим становится актуальной задача обеспечения надежности ИУС с помощью проведения обновлений ПС.

Целью статьи является разработка метода обеспечения надежности распределенных ИУС с учетом повышения безотказности ПС в процессе их обновления. Для этого необходимо:

– принять основные допущения для определения входных параметров метода обеспечения заданных показателей надежности ИУС;

– разработать последовательность анализа надежности распределенных ИУС с учетом отказов, вызванных проявлением различных видов неисправностей;

– на основе полученных в ходе анализа надежности данных, выработать рекомендации по обеспечению заданных показателей надежности распределенных ИУС;

– провести анализ достоинств и недостатков метода обеспечения надежности распределенных ИУС и сделать выводы о перспективе дальнейших исследований в заданном направлении.

Основные допущения, принимаемые в процессе обеспечения заданных показателей надежности распределенных ИУС

В процессе обеспечения надежности распределенных ИУС принимаются следующие допущения:

– аппаратная и программная компоненты ИУС собираются из универсальных составляющих, которые прошли этапы тестирования и верификации;

– потоки событий, переводящие систему из одного функционального состояния в другое, обладают свойствами стационарности, ординарности и отсутствием последействия;

– каждый элемент ИУС в произвольный момент времени может находиться либо в работоспособном, либо в неработоспособном состоянии;

– нарушение работоспособного состояния АС ИУС вызвано физическими дефектами (ДФ АС) [2, 3];

– нарушение работоспособного состояния ПС ИУС может быть вызвано дефектами проектирования (ДП) [3, 7], случайными ошибками обслуживающего персонала и пользователей (СО) [7, 10] и злонамеренными действиями обслуживающего персонала и пользователей (ЗД) [10];

– стоимость обновления ПС намного меньше закупки и использования программной продукции другого разработчика для организации диверсной системы.

Применение распределенной структуры построения ИУС позволяет проводить мероприятия ТО без нарушения работоспособного состояния системы в целом. Однако некоторые мероприятия, например, обновление версии программ в процессе их сопровождения, требуют пусть даже кратковременного, но все-таки простоя системы. Эти особенности необходимо учитывать при обеспечении заданных показателей надежности. Поэтому в работе рассматривается два вида обновлений ПС:

– обновления ПС ИУС первого рода, которые проводятся периодически (например, смена версии ПС) и предусматривают простой системы на протяжении процедур обновления;

– обновления ПС ИУС второго рода, которые проводятся через некоторое время после обнаружения ошибки, дефекта, неисправности или «дыры» в программе (например, установка «patches»-заплат) и предусматривают простой только одного из элементов ИУС, а не системы в целом.

Этапы анализа надежности распределенных ИУС с учетом отказов, вызванных проявлением различных видов неисправностей

Предварительный анализ надежности позволяет определить степень несоответствия требуемым значениям показателей надежности проектируемой ИУС с выбранной структурой и параметрами обновлений ПС. В основу мероприятий анализа надежности распределенных ИУС положен аппарат марковских однофрагментных (статических) моделей [3] и регулярных многофрагментных моделей (РМФМ) (динамические модели) [8].

Основные этапы анализа надежности распределенных ИУС следующие (алгоритм метода обеспечения надежности приведен на рис. 1).

1. Анализ документации на исследуемую систему (техническое задание, технические условия, инструкция по эксплуатации, нормативные документы и др. доступные источники). При этом выявляются все требования к системе (оператор 1), производится выбор одной из базовых распределенных структур и способа обновлений ПС (оператор 2). Также возможен вариант начального применения нераспределенной структуры без обновлений ПС.

2. Обоснование возможности описания функционирования ИУС как марковского случайного процесса. Закон распределения времени между отказами элементов ИУС экспоненциальный. Это дает возможность рассматривать случайный процесс, протекающий в ИУС, как марковский процесс с дискретными состояниями и непрерывным временем. В случае если в процессе функционирования ИУС производятся обновления ПС, необходимо обосновать возможность описания процесса функционирования ИУС аппаратом регулярных многофрагментных моделей [8] (принятие основных допущений, оператор 3).

3. На основании определенных в документации критериев отказа и выбранной структуры системы построить структурную схему надежности ИУС с учетом всех распределенных элементов (оператор 4). По ССН построить размеченный граф состояний и переходов системы $G(V, N)$ (оператор 5), где $V = M\{v_i\}$ – множество вершин (состояния ИУС), $N = M\{n_{ij}\}$ – множество дуг (условных плотностей распределений вероятностей отказов и восстановлений, определяющих переход из одного состояния в другое). Набор состояний графа $G(V, N)$ представляет собой полную группу событий.

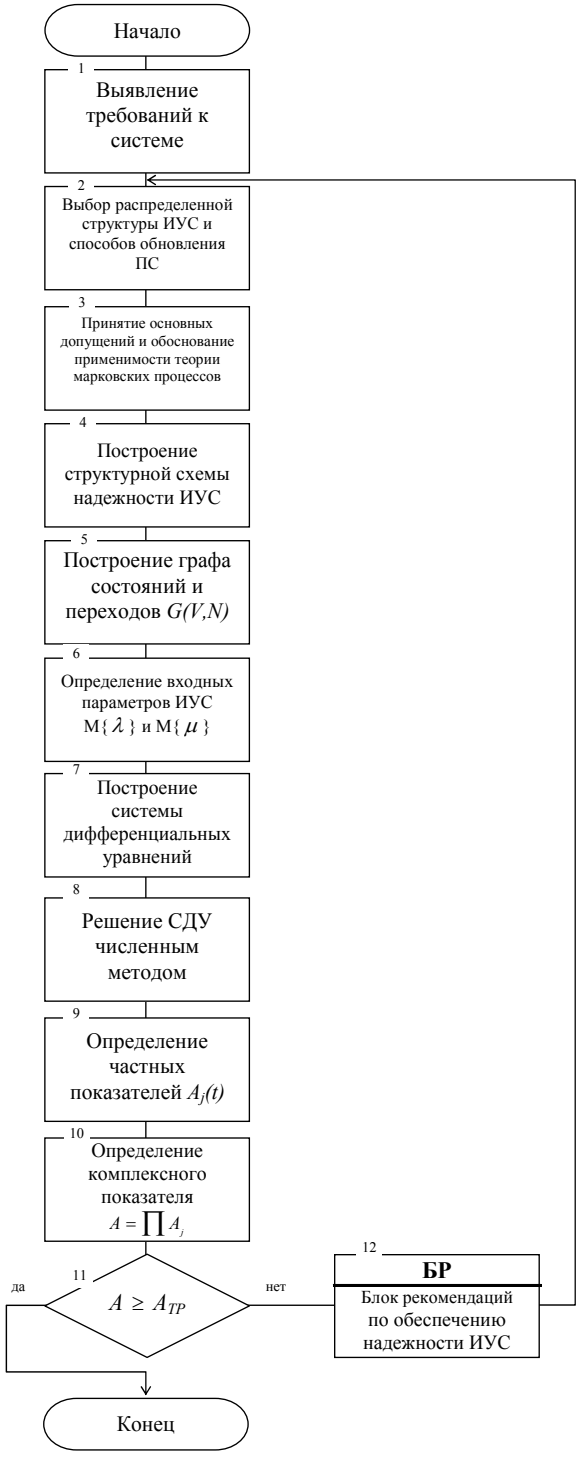

Рис. 1. Алгоритм метода обеспечения надежности распределенных ИУС

4. Для учитываемых видов неисправностей из доступных источников осуществляется определение количественных значений параметров, позволяющих определить вероятностно-временные показатели надежности (параметры интенсивностей отказов и восстановлений элементов ИУС) (оператор 6).

В случае отсутствия количественных данных о параметрах АС ИУС осуществляется расчет значений интенсивностей отказов и восстановлений АС элементов ИУС на основании наиболее приемлемых моделей безотказности и ремонтопригодности АС, (например [3, 5]).

В случае отсутствия количественных данных о параметрах ПС ИУС осуществляется расчет значений интенсивностей проявления ДП, СО и ЗД и интенсивностей восстановления ПС элементов ИУС на основании моделей надежности [7, 10]. Для ИУС, в которых проводятся обновления ПС, необходимо определить интенсивность проведения обновлений ПС и интенсивность восстановления системы после проведения обновления ПС [7].

5. По графу состояний и переходов определить систему дифференциальных уравнений (СДУ) Колмогорова [3]. При этом каждому состоянию S_i графа G ставится в соответствие $P_i(t)$ – вероятность нахождения ИУС в i-м состоянии (оператор 7). Для многофраментных моделей СДУ будет состоять из последовательности регулярных блоков, описывающих фрагменты РМФМ.

6. Для различных параметров размеченного графа состояний и переходов выполнить операторы 8 и 9. Для решения полученной СДУ численным методом (например, экспоненциальным [11]) необходимо синтезировать квадратную разреженную матрицу коэффициентов с учетом количественных значений параметров системы. После решения СДУ (оператор 8) необходимо определить частные показатели надежности $A_j(t)$ (комплексные показатели надежности ИУС с учетом проявления только одного вида неисправностей, например ДП) как вероятности нахождения системы на множестве работоспособных состояний (оператор 9).

7. Определить значение полного показателя надежности $A(t)$ (комплексного показателя надежности с учетом проявления всех рассматриваемых видов неисправностей: ДФ АС, ДП, СО и ЗД) из выражения (оператор 10):

$$A(t) = \prod A_j(t) \qquad (1)$$

8. Сравнить полученное значение $A(t)$ с требуемым (оператор 11). В случае положительного ответа делается вывод о соответствии выбранной структуры ИУС и проводимой политики обновлений ПС ИУС требованиям, выдвигаемым к системе. В случае отрицательного ответа делается вывод о несоответствии ИУС выдвигаемым требованиям. После этого выполняются рекомендации по обеспечению надежности ИУС (оператор 12).

Далее производится повторная оценка соответствия надежности ИУС заданным требованиям (переход к оператору 2).

Таким образом, последовательность мероприятий по обеспечению надежности выполняется циклически до того момента, когда ИУС будет отвечать выдвигаемым требованиям.

Рекомендации по обеспечению заданных показателей надежности распределенных ИУС

В связи с тем, что существует несколько способов повышения надежности распределенных ИУС, при разработке рекомендаций необходимо учитывать экономический аспект проводимых мероприятий обеспечения заданных показателей надежности.

В основу рекомендаций по обеспечению надежности распределенных ИУС положен анализ полученных результатов оценки частных показателей надежности на минимальные значения. На основании проведенного анализа выявляются наиболее критичные виды неисправностей системы (те виды, для которых показатель $A_j(t)$ имеет минимальное

значение). Кроме того, необходимо учитывать виды обновлений ПС, которые проводятся или не проводятся в рассматриваемой ИУС.

В связи с этим комплекс мероприятий по обеспечению заданных показателей надежности ИУС представлен в табличной форме (табл.2).

Таблица 2

Комплекс мероприятий по обеспечению надежности распределенных ИУС

<table>
<tr><td rowspan="2">Наиболее критичный вид неисправностей по показателю A_j</td><td colspan="3">Характер проведения обновлений ПС ИУС на начальном этапе</td></tr>
<tr><td>Обновления ПС ИУС не проводятся</td><td>Проводятся обновления ПС ИУС первого рода</td><td>Проводятся обновления ПС ИУС второго рода</td></tr>
<tr><td>ЗД</td><td>Проводить обновления ПС второго рода</td><td rowspan="2">1 этап. Увеличить количество (периодичность) обновления ПС первого рода, учитывая при этом увеличение суммарного времени простоев системы.
2 этап. Руководствуясь экономическими критериями либо перейти к эксплуатации ПС, допускающих обновления второго рода, либо увеличить диверсность ПС ИУС</td><td rowspan="2">1 этап. Увеличить интенсивность обновлений ПС второго рода.
2 этап. Увеличить диверсность ПС ИУС</td></tr>
<tr><td>ДП</td><td>Проводить обновления ПС первого рода</td></tr>
<tr><td>ДФ АС, СО</td><td colspan="3">Увеличить степень распределения (количество распределенных элементов) ИУС</td></tr>
</table>

После выполнения любой из рекомендаций по обеспечению надежности ИУС производится повторная оценка полного комплексного показателя надежности согласно последовательности, изображенной на рис. 1. Поэтому рекомендации, указанные в табл. 2, носят последовательный характер. Например, если в ИУС не проводятся обновления ПС, и в ходе анализа выяснилось, что наиболее критичный вид неисправностей – ДП, то рекомендуется проводить обновления первого рода. Если при повторном анализе надежности выяснилось, что проведение обновлений первого рода не позволяет обеспечить заданные значения показателей надежности ИУС, то выполняются рекомендации первого этапа из соответствующего столбца таблицы (3-го по счету). Если последующий анализ надежности показал, что увеличение количества обновлений ПС первого рода не позволяет обеспечить требуемую надежность ИУС, то выполняются рекомендации второго этапа этого же столбца (3-го по счету) табл. 2.

Допустим, выполнен переход к эксплуатации ПС, для которых проводятся обновления второго рода. Если последующий анализ надежности показал, что выполненные рекомендации и рекомендации первого этапа 4-го столбца табл. 2 не позволяют обеспечить требуемую надежность ИУС, то выполняется выбор диверсной структуры системы согласно [3, 9], что является наиболее дорогим решением проблемы обеспечения надежности ИУС.

В случае выполнения заданных требований цель работ по оценке и обеспечению надежности распределенных ИУС считается выполненной.

Заключение

Дальнейшее развитие метода обеспечения надежности распределенных ИУС позволяет обеспечить заданные показатели надежности не только с помощью структурной избыточности и диверсности ПС, но и изменением параметров обновлений ПС системы.

Представленный в статье метод позволяет выделить последовательности рекомендаций по обеспечению надежности ИУС, условно сгруппированные табличную форму (табл. 2).

В представленном методе конкретизированы ме-

роприятия по предотвращению определенных видов неисправностей распределенных ИУС, что позволяет сократить суммарное время определения значений параметров ИУС, при которых система будет удовлетворять заданным показателям надежности.

В ряде случаев применение обновлений ПС позволяет уменьшить расходы на обеспечение заданных показателей надежности по сравнению с традиционными методами повышения структурной и диверсной избыточности.

В соответствии с предложенным методом обеспечения оценки надежности распределенных ИУС дальнейшие исследования следует направить на разработку и усовершенствование методов приближенной оценки параметров системы, при которых выполняются заданные требования к надежности ИУС.

Литература

1. High-Availability Computer Systems / J. Gray, D.P. Siewiorek // IEEE Computer. – 1991. – Vol. 9. – P. 39 – 48.

2. Basic concepts and taxonomy of dependable and secure computing / A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on dependable and secure computing. – 2004. – № 1. – P. 11 – 33.

3. Харченко В.С., Тимонькин Г.Н., Сычев В.А. Основы построения и проектирования АСУ техническим состоянием летательных комплексов. Ч. 1. Основы теории надежности и управления техническим состоянием летательных комплексов: Учебн. пос. – Х.: ХВКИУ, 1992. – 276 с.

4. Дружинин Г.В. Надежность автоматизированных систем. Изд. 3-е перераб. и доп. – М.: Энергия, 1977. – 536 с.

5. MIL-HDBK-338B. Military handbook. Electronic reliability design handbook. Int. 1.10.98 – DoD. 1998. – 1046 p.

6. Modeling and Analysis of Software Rejuvenation in Cable Modem Termination System / Y. Liu, Y. Ma, J.J. Han, H. Levendel, K.S. Trivedi // Proceedings of the 13th Int'l. Symposium on Software Reliability Engineering. ISSRE. 2002. – P. 159 – 170.

7. Поночовный Ю.Л., Одарущенко Е.Б. Моделирование надежности обновляемых программных средств нерезервированных информационно-управляющих систем постоянной готовности // Радіоелектронні і комп'ютерні системи. – 2004. – Вип. 4 (8). – С. 93 – 97.

8. Оценка надежности программно-технических комплексов на основе многофрагментных марковских моделей / Е.Б. Одарущенко, О.Н. Одарущенко, А.В. Стороженко, П.Н. Гроза // Системи обробки інформації.– Х.: ХВУ. – 2001. – Вип. 10 (38). – С. 110 – 116.

9. Скляр В.В. Анализ метрик диверсности программного обеспечения // Электронное моделирование. – 2004. – Вип. 26. – С. 95 – 104.

10. Поночовный Ю.Л. Определение параметров закона распределения времени между отказами восстанавливаемых обслуживаемых многопользовательских систем с учетом дефектов взаимодействия // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 10 (38). – С. 166 – 174.

11. Одарущенко О.Н., Одарущенко Е.Б., Поночовный Ю.Л. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем // Авіаційно-космічна техніка і технологія. – Х.: Нац. аерокосм. ун-т «ХАІ». – 2002. – Вип. 3. – С. 187 – 191.

Поступила в редакцию 12.10.2005

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.