

УДК 004.052.3

**В.А. Михеев**

### **СИСТЕМНЫЙ АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ И ПОВЫШЕНИЯ НАДЕЖНОСТИ МНОГОФУНКЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

*Рассмотрена проблема обеспечения и повышения надежности многофункциональной информационной системы холдинга, вследствие возникновения угроз потери или модификации (искажения) информации, циркулирующей в системе. Проведен анализ существующих подходов и методов обеспечения и повышения надежности комплексов программных и технических средств. Обоснована необходимость использования методов повышения надежности, в зависимости от этапа жизненного цикла многофункциональной информационной системы. На основе этих методов выработаны и проанализированы направления и принципы обеспечения и повышения надежности функционирования многофункциональной информационной системы.*

*Информационная система; надежность; отказ; избыточность.*

**V.A. Mikheev**

### **SYSTEM ANALYSIS OF METHODS TO PROVIDE AND INCREASE RELIABILITY OF MULTIFUNCTIONAL INFORMATION SYSTEM**

*The article describes the problem to provide and increase the reliability of multifunctional information system of the holding company as there is a threat of loss and garbling of the information circulated in the system. The existing approaches and methods to provide and increase the reliability of bundled software and hardware are analyzed. It is justified that the methods to increase the reliability need to be used depending on the life cycle phase of multifunctional information system. Based on these methods the directions and the principles to provide and increase the reliability of multifunctional information system operation have been developed and analyzed.*

*Information system; reliability; failure; redundancy.*

Многофункциональная территориально распределенная информационная система (МИС) – взаимосвязанная совокупность кампусных локальных вычислительных сетей (ЛВС) и сетей передачи данных, предназначенная для создания единого защищенного интегрированного информационного пространства информационных ресурсов предприятий холдинга. Многофункциональность системы определяется наличием в ней целого ряда функциональных систем и подсистем, а также комплексов технических и программных средств (КТС и КПС).

По мере развития МИС и усложнения используемых программно-аппаратных средств происходит повышение уязвимости МИС. Основными факторами, способствующими повышению уязвимости, являются:

- увеличение объемов информации, хранимой, обрабатываемой и передаваемой в МИС;

- расширение круга пользователей, имеющих непосредственный доступ в соответствии с ролями и полномочиями доступа к ресурсам МИС;
- сосредоточение в единой базе данных разнородной информации;
- усложнение режимов функционирования МИС, связанных с непрерывной обработкой данных.

Таким образом, возникает угроза потери или модификации (искажения) информации, циркулирующей в МИС. В связи с этим проблема обеспечения качества и необходимость повышения надежности системы приобретают ключевой характер на всех этапах жизненного цикла системы [1]. Общие требования по надежности могут быть определены в зависимости от принадлежности МИС к определенному классу ИС (табл. 1).

Таблица 1

#### Классификация ИС по коэффициенту готовности

Коэффициент готовности, %	Максимальное время простоя	Класс ИС
99,0	3,65 дня/год	Обычная (Conventional)
99,9	43,8 минуты/месяц или 8,76 часов/год	Высокой готовности (High Availability)
99,99	4,38 минуты/месяц или 52,6 минуты/год	Отказоустойчивая (Fault Resilient)
99,999	0,44 минуты/месяц или 5,26 минуты/год	Безотказная (Fault Tolerant)
99,9999	31,54 секунды/год	Непрерывной готовности (Continuous Availability)

**Классификация ИС по требованиям надежности.** Классификация ИС по требованиям надежности основана на значении коэффициента готовности, который определяется как отношение времени, проведенного системой в работоспособном состоянии, к общему времени работы:

$$K_{\text{г}} = \frac{l_p}{T_p + T_E} * 100\% , \quad (1)$$

где  $T_p$  – время работы системы без отказов,

$T_E$  – время восстановления системы после отказа.

Значение коэффициента готовности находится в диапазоне от 99 до 99,9(9) %, в зависимости от класса (типа) ИС (табл. 1).

Рассмотрим подробнее особенности существующих классов ИС, позволяющих обеспечить значение коэффициента готовности равным 99,9 % и выше [2].

**Системы высокой готовности (High Availability).** Такие системы для минимизации планового и unplanned времени простоя используют обычные программно-аппаратные технологии. При этом конфигурация системы обеспечивает ее быстрое восстановление после обнаружения неисправности, для чего используются избыточные технические и программные средства. Длительность задержки, в

течение которой программа, отдельный компонент или система простаивает, может находиться в диапазоне от нескольких секунд до нескольких часов.

**Отказоустойчивые системы (Fault Resiliency).** Особенностью ИС этого типа является более короткое время восстановления, которое позволяет системе быстро откатиться на шаг назад, после обнаружения неисправности.

**Безотказные системы (Fault Tolerance).** Такие ИС имеют в своем составе избыточную аппаратуру для всех функциональных блоков, включая процессоры, источники питания, подсистемы ввода/вывода, дисковой памяти и т.д. Если соответствующий функциональный блок неправильно функционирует, всегда имеется горячий резерв. Время восстановления после обнаружения неисправности для переключения отказавших компонентов на избыточные для таких систем обычно одна-две секунды.

**Системы непрерывной готовности (Continuous Availability).** Такая система устраняет время простоя как плановое, так и неплановое. Разработка такой системы охватывает как аппаратные, так и программные средства и позволяет проводить модернизацию и обслуживание системы в режиме on-line. Время восстановления после обнаружения неисправности не превышает одной секунды.

На основе ряда публикаций [2, 9 – 11] и комментариев экспертов можно сделать вывод, что требования по надежности для современных ИС за последние 10 – 15 лет неуклонно растут. Этот факт привел к появлению нового класса ИС – систем, устойчивых к стихийным бедствиям и катастрофам (Disaster Tolerance). Для такого класса систем значение коэффициента готовности должно вычисляться способами, отличными от (1), и в этой связи в общую классификацию этот тип систем не включен. Катастрофоустойчивые системы имеют возможность перезапуска или продолжения своих функций на другой (резервной) территориально удаленной площадке, если основное месторасположение системы оказывается в нерабочем состоянии, то есть устойчивость к стихийным бедствиям и катастрофам требует полного (зеркального) дублирования ИС вне основного местоположения, позволяющего принять на себя работу немедленно после отказа системы на основной площадке.

В целом для рассматриваемой МИС (в зависимости от подсистем и выполняемых функций) характерны требования по надежности с коэффициентом готовности 99,9 %, что позволяет отнести МИС к классу систем высокой готовности, однако отдельные подсистемы МИС можно отнести и к более высоким классам – отказоустойчивым системам.

В теории надежности существует единая установившаяся терминология, охватывающая важнейшие понятия и определения, подробно изложенные в ряде национальных стандартов [3 – 5]. Надежность МИС является одной из основных составляющих её качества. Качество – совокупность свойств продукции, которая позволяет оценить пригодность продукции удовлетворять определенным потребностям в соответствии с её назначением (рис. 1).

В соответствии с [3] надежность трактуется как свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортирования. Необходимо отметить, что надежность является комплексным свойством системы и включает в себя еще четыре свойства (рис. 1):

- безотказность – свойство системы не утрачивать работоспособность в течение заданной наработки без перерывов;

- долговечность – свойство системы сохранять работоспособность до предельного состояния (до списания) с перерывами на техническое обслуживание и ремонт;
- ремонтпригодность – свойство системы обнаруживать, устранять и предупреждать неисправность и отказы путем проведения технического обслуживания и ремонта;
- сохраняемость – свойство системы сберечь свои эксплуатационные показатели в течение и после срока транспортирования или хранения на складе.

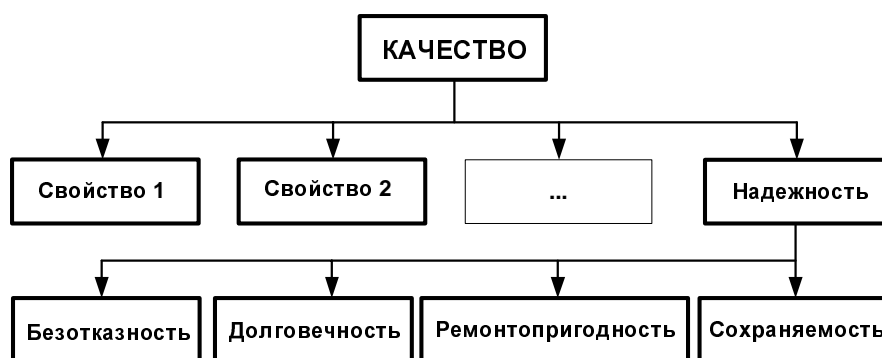


Рис. 1. Структура свойств качества и надежности

Под надежностью МИС понимается её защищенность от случайных или преднамеренных вмешательств в нормальный процесс её функционирования, выражающаяся в потере или модификации (искажении) информации.

К угрозе потери или модификации (искажения) информации приводят отказы и сбои (самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора) в работе МИС.

Классифицировать отказы можно в зависимости от характера и особенностей, от момента возникновения, например, следующим образом [6].

По характеру изменения параметра до момента возникновения отказа:

- внезапный отказ;
- постепенный отказ.

По связи с другими отказами:

- независимый отказ;
- зависимый отказ.

По возможности последующего использования после возникновения отказа:

- полный отказ;
- частичный отказ.

По характеру устранения отказа:

- устойчивый отказ;
- самоустраняющийся отказ (сбой или перемежающийся отказ).

По наличию внешних проявлений:

- очевидный (явный) отказ;
- скрытый (неявный) отказ.

По причине возникновения:

- конструкционный отказ;

- технологический отказ;
- эксплуатационный отказ.

По природе происхождения:

- естественный отказ;
- искусственный отказ (вызываемый намеренно).

По времени возникновения отказов:

- отказ при испытаниях;
- отказ периода приработки;
- отказ периода нормальной эксплуатации;
- отказ последнего периода эксплуатации.

Необходимо отметить, что отказы можно отнести к конструкционным, технологическим или эксплуатационным, с целью установления, на каком этапе жизненного цикла МИС следует провести мероприятия, предупреждающие и устраняющие причины возникновения отказов.

Применительно к рассматриваемой системе, отказы можно разбить на две группы [6]:

- нарушения в работе комплекса технических средств (КТС) – аппаратный отказ/сбой;
- нарушения в работе комплекса программных средств (КПС) – программный отказ/сбой.

Для обеспечения требований по надежности в соответствии с классом МИС, необходимо применение методов обеспечения и повышения надежности как КТС, так и КПС.

**Методы повышения надежности КТС.** В настоящее время известно множество различных методов повышения надежности КТС ИС, однако не все из них могут найти применение в рамках рассматриваемой системы.

Исходя из этого, применимые для МИС методы повышения надежности КТС можно ограничить разбивкой на четыре группы:

- введение избыточности КТС (структурной, информационной, временной, функциональной, алгоритмической);
- применение более надежных компонентов;
- улучшение условий эксплуатации;
- организация интенсивного профилактического обслуживания как всей системы, так и отдельных ее элементов.

Рассмотрим основные виды избыточности КТС первой группы.

Структурная избыточность (или аппаратная) предусматривает использование избыточного КТС. Суть такого вида резервирования заключается в том, что в минимально необходимый вариант системы, элементы которой называют основными, вводятся дополнительные элементы, узлы, устройства либо даже вместо одной системы предусматривается использование нескольких идентичных систем. При этом избыточные структурные элементы, узлы, устройства и т.д. предназначены для выполнения рабочих функций при отказе соответствующих основных элементов, узлов и устройств.

Информационная избыточность предусматривает использование избыточной информации. Простейшим примером реализации такого вида избыточности является многократная передача одного и того же сообщения по каналу связи, а также использование специальных кодов, обнаруживающих и исправляющих ошибки (коды с повторением и инверсией, циклический код, код Хемминга и т.д.), которые появляются в результате сбоев и отказов. Здесь следует заметить, что использова-

ние информационной избыточности влечет за собой также необходимость введения избыточных технических средств.

Временная избыточность предусматривает использование избыточного времени. В случае применения этого вида резервирования предполагается возможность возобновления функционирования системы после того, как оно было прервано в результате отказа, путем его восстановления. При этом также предполагается, что на выполнение необходимой работы отводится время, заведомо большее минимально необходимого.

Функциональная избыточность предусматривает, что при отказе отдельных элементов, функции системы перераспределяются между работающими, таким образом, исправные элементы начинают работать более интенсивно.

Алгоритмическое резервирование. Алгоритмы, используемые в вычислительной системе, содержат избыточное количество операторов для преодоления сбоев и отказов.

Применение второй группы методов избыточности не позволит обеспечить необходимый уровень надежности МИС, вследствие того, что он требует применения фактически нового КТС (имеющего более высокие показателями надежности) и значительного увеличения финансовых затрат.

Третья группа методов предполагает приведение условий эксплуатации КТС в соответствие с требованиями, при которых гарантируются паспортные данные технических средств по надежности. Дальнейшее же улучшение условий эксплуатации не может существенно повысить надежность функционирования КТС.

Четвертая группа методов предполагает организацию профилактического обслуживания КТС (совокупность плановых мероприятий, проводимых на работоспособных элементах и повышающих их надежность) – мониторинг и выявление сбойных элементов, их восстановление или замену новыми.

Очевидно, что методы первой и второй групп необходимо реализовывать на этапе разработки МИС, а третьей и четвертой – на этапе эксплуатации.

Таким образом, основным методом повышения надежности КТС на этапе разработки МИС является применение структурной избыточности. Другие виды избыточности (временная, алгоритмическая и т.д.) также могут применяться, но параллельно и в качестве дополнительных к структурному резервированию.

Структурная избыточность вводится в КТС с целью улучшения надежностных характеристик и показателей. В настоящее время известно много методов целенаправленного введения структурной избыточности (горячее и холодное резервирование, мажоритарные структуры и т.п.), что позволяет обеспечить требуемый уровень надежности МИС на основе применения ненадежных элементов.

Основной недостаток подхода на основе структурной избыточности – значительное увеличение количества (в зависимости от объемов и кратности резервирования) технических средств и общей стоимости проектных решений, не гарантирующее при этом пропорциональный рост надежности системы в целом.

**Методы повышения надежности КПС.** Как ранее было отмечено, надежность МИС определяется не только отказами КТС, но и отказами КПС, вызываемыми ошибками в программах. Если отказы КТС зависят от времени и не зависят от обрабатываемой информации, то отказы КПС, наоборот, не зависят от времени, зато зависят от обрабатываемой информации, а также от текущего состояния ИС.

Оценка надежности КПС может быть получена непосредственно на основе свойств используемого в рамках МИС программного обеспечения (ПО).

Для сокращения до минимума количества ошибок, встречающихся в ПО, необходимо анализ совокупности факторов, определяющих надежность ПО, которые можно разделить на три группы [7, 8, 9]:

- общие факторы;
- факторы, связанные с разработкой ПО;
- эксплуатационные факторы.

К общим факторам относятся:

- процедуры управления разработкой ПО;
- подготовка управления разработкой ПО;
- архитектура вычислительной системы;
- языки программирования.

К факторам, связанным с разработкой ПО, относятся:

- конструктивные (стоимость разрабатываемой системы, структура построения программы, наличие опыта разработки, степень соблюдения последовательности работ);
- технологические (техника программирования);
- организационные (контроль и управление надежностью в процессе разработки, степень обучения и информативности персонала, микроклимат в группе, выполняющей разработку, временные ограничения на выполнение работ).

К эксплуатационным факторам относятся:

- полнота и качество эксплуатационной документации;
- степень адаптации документации;
- простота изучения и использования системы ПО;
- качество обучения пользователей, ответственных за эксплуатацию ПО;
- степень выполнения стандартов на эксплуатацию ПО.

Для достижения заданного уровня надежности КПС необходимо [6,7,11]:

- избегать ошибок, возникающих в процессе создания ПО;
- обнаруживать ошибки;
- исправлять допущенные ошибки;
- предусматривать возможность наличия ошибок.

К средствам избегания ошибок в процессе проектирования относятся такие, целью которых является предупреждение появления ошибок в программе, а именно:

- средства и приемы минимизации сложности как основной причины ошибок трансляции;
- средства и методы совершенствования информационных связей разработчиков;
- средства и приемы немедленного обнаружения и удаления ошибок трансляции после каждого ее шага, а не после завершения написания программы.

К средствам обнаружения ошибок относятся:

- организация проверки значений входных данных на известное ограничение;
- проверка на совместимость входных данных;
- введение необходимой избыточности входных данных;
- организация сравнения входных данных с некоторым набором внутренних данных.

Эффективные средства автоматического исправления ошибок в ПО ещё не разработаны, однако судя по публикациям, исследования в этой области ведутся непрерывно.

Средства допущения ошибок обеспечивают возможность функционирования ПО в случае, когда в нем присутствуют ошибки. В составе этих средств можно выделить динамическую избыточность, вспомогательные методы и изоляцию ошибок [8 – 10].

Очевидно, что при прочих равных условиях (квалификация разработчиков, период эксплуатации, устранение ошибок после их обнаружения и т.д.) через некоторый промежуток времени функционирование более надежным становится ПО массового использования (постоянный и своевременный выход патчей, обновлений и т.д.).

Следовательно, для повышения надежности КПС МИС необходимо применять ПО массового использования, а разработку собственного ПО вести с учетом рассмотренной совокупности факторов, определяющих надежность ПО.

Обеспечение надежности МИС требует решения множества научно-технических проблем. При минимизации применения в МИС ПО собственной разработки, проблема повышения надежности КТС имеет больший приоритет, по сравнению с проблемой повышения надежности КПС, а основным методом повышения надежности КТС является метод применения структурной избыточности, при этом другие рассмотренные методы повышения надежности также могут быть использованы в качестве дополнительных к основному.

Также необходимо решить задачу синтеза рациональной структуры и выбора наиболее эффективных технических решений построения МИС, в которой помимо достижения заданных показателей по надежности обеспечивается поддержание требуемого уровня защищенности.

#### БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Михеев В.А.* Методология разработки и аттестации автоматизированных систем в защищенном исполнении // Материалы IX Международной научно-практической конференции «Информационная безопасность-2007». Ч. 1. – Таганрог 2007.
2. *Шнитман В.* Современные высокопроизводительные компьютеры // Информационно-аналитические материалы Центра информационных технологий [Электронный ресурс]. – Режим доступа: <http://www.fizmat.vspu.ru/citforum/hardware/svk/contents.shtml>. Дата обращения 01.09.2009.
3. ГОСТ 27.001-95. Система стандартов "Надежность в технике". Основные положения. Введ. с 01.01.1997. – М., 1995. – 7 с.
4. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. Введ. с 01.07.1990. – М., 1990. – 24 с.
5. ГОСТ 27.003-90. Состав и общие правила задания требований по надежности. Введ. с 01.01.1992. – М., 1991. – 17 с.
6. *Морозов Ю. Д., Ильин И. И.* Методы обеспечения качества и надежности проектов автоматизированных систем. – М.: МЭСИ, 1990. – 110 с.
7. *Майерс Г.* Надежность программного обеспечения. – М.: Мир, 1980. – 360 с.
8. *Леонтьев Е.А.* Надежность экономических информационных систем. – Тамбов: ТГТУ, 2002. – 128 с.
9. *Кульба В.В., Ковалевский С.С., Шелков А.Б.* Достоверность и сохранность информации в АСУ. – М.: СИНТЕГ, 2003. – 500 с.
10. *Дружинин Г.В.* Надежность автоматизированных производственных систем: – М.: Энергоатомиздат, 1986. – 480 с.



11. *Зиновьев П.А., Моисеев В.С., Мейко А.В.* Модели для оценки надежности архитектурных решений корпоративных систем хранения данных // Исследования по информатике. – Казань: Отечество, 2005. Вып. 9. – С. 93 – 102.

**Михеев Вячеслав Алексеевич**

Открытое акционерное общество «Концерн радиостроения “Вега”».  
E-mail: mikheev@vega.su.  
121170, г. Москва, Кутузовский проспект, 34.  
Тел.: 8 (499) 2490585.  
Заместитель директора.

**Mikheev Viatcheslav Alekseevich**

Joint-Stock Company «Radio Engineering Corporation “VEGA”».  
E-mail: mikheev@vega.su.  
34, Kutuzov avenue, Moscow, 121170, Russia.  
Phone: 8 (499) 2490585.  
The deputy director.

УДК 530.1:537.86

**И.И. Маркович, В.Ю. Дорошенко**

**ИССЛЕДОВАНИЯ АЛГОРИТМОВ ОБНАРУЖЕНИЯ БИООБЪЕКТОВ ЗА ПРЕПЯТСТВИЯМИ СВЕРХШИРОКОПОЛОСНЫМ РАДАРМ**

*Рассматриваются алгоритмы цифровой обработки сверхширокополосных сигналов в радарх для обнаружения биологических объектов за препятствиями. Представлены результаты экспериментальных исследований возможности обнаружения объектов за препятствиями из кирпича, бетона, армированного бетона.*

*Сенсорная сеть; сверхширокополосные сигналы; обнаружение биологических объектов за препятствиями; СШП-радиолокаторы; цифровая обработка сигналов; алгоритмы цифровой высокочастотной фильтрации.*

**I.I. Markovich, V.U. Doroshenko**

**ANALYSIS OF ALGORITHMS DETECT ION BIOLOGICAL OBJECT AFTER OBSTACLES OF ULTRA BANDWIDTH RADAR**

*This article is devoted to digital signal processing algorithms of UWB radar signals for detection of biological object after obstacles. Presented are the experimental research results possibilities to detect biological objects after bricks, concrete and reinforced concrete obstacles.*

*Net of sensor; ultra bandwidth signal; detection of biological object after obstacles; UWB radar systems; digital signal processing; high-frequency filtration algorithms.*

Проблема оперативного обнаружения людей за препятствиями из кирпича, бетона или армированного бетона становится особенно актуальной при проведении спасательных и антитеррористических операций. Создание сверхширокополосных (СШП) радаров, предназначенных для обнаружения биологических объек-