УДК 004.052

АНАЛИЗ ПРОБЛЕМ НАДЕЖНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Хаданова К.В., Цыганцев Д.А., студенты гр. ПИм-191, I курс
Научный руководитель: Крюкова В.В., к.т.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

Для современных информационных систем одними из самых важных проблем являются проблемы надежности. Их решение во многих случаях определяет, будет ли существовать система. К таким системам относятся различные системы мониторинга, территориально распределенные системы, информационные системы с большим количеством узлов и сетевой структурой и т.д.

Растет сложность информационных систем, в их составе используется всё больше уникального ПО, кроме того, в процессе управления, обработки и передачи информации принимает участие человек [1]. Всё это требует прогнозирования надежности систем, разработки устойчивых методов расчета и использования соответствующих технических средств.

Кроме того, усложнение происходит в различных направлениях. Во-первых, происходит увеличение количества компонентов систем, а во-вторых, становится более сложной их структура, определяющая взаимодействие в рабочем процессе и сохранении рабочего состояния, а также соединение отдельных компонентов. Такое усложнение происходит из-за того, что увеличивается многообразие, важность и трудоемкость функций, которые выполняются системами.

В то же время, системы, отличающиеся большей сложностью, включающие большее количество компонентов и имеющие более сложные алгоритмы работы, являются менее надежными в сравнении с более простыми системами. В связи с этим возникает необходимость разработки специализированных методов обеспечения надежности, включая разработку математических методов расчета надежности и экспериментальных оценок [2].

Целью данной работы является анализ и структуризация проблем надежности, а также методов их решения.

Понятию «распределенная система» дано множество определений. Наиболее полное из них предложил А.С. Таненбаум [3]: «Распределенная система (РС) – это набор независимых компьютеров, который воспринимается его пользователям как единственная последовательная система». Существует и другое определение [4]: распределенными системами называются програм-

мно-аппаратные системы, в которых исполнение операций (действий, вычислений), необходимых для обеспечения целевой функциональности системы, распределено (физически или логически) между разными исполнителями.

Распределенные системы должны быть [5]: прозрачными, открытыми, безопасными, масштабируемыми и надежными. Рассмотрим надежность более подробно.

ГОСТ 27.002-89 определяет надежность следующим образом – это свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания и транспортирования.

Многие системы абсолютно надежными не являются, так как свойство надежности системы сохраняется лишь на конечном интервале времени, по истечении которого в работе может произойти отказ. Его обычно считают случайным событием, потому что длительность интервала безотказной работы зависит от очень большого числа факторов, предсказать которые невозможно.

Основной параметр, по которому определяют надежность РС – отказоустойчивость [5]. Это одно из важнейших свойств вычислительной системы, позволяющее продолжать работу после появления неполадок.

Надежность принято характеризовать значением вероятности появления отказа в работе (или вероятностью безотказной работы) за конкретный непрерывный отрезок времени [6]. Еще одна характеристика надежности – среднее время наработки на отказ.

Систему можно считать надёжной в том случае, когда применительно к ней соблюдаются некоторые требования:

1. Доступность – свойство быть в работоспособном состоянии в любой момент.
2. Безопасность – определение, насколько катастрофической становится ситуация в случае остановки системы.
3. Ремонтопригодность – оценка сложности исправления возникших ошибок, в том числе при наличии средств их автоматического обнаружения и исправления.
4. Избыточность – один из способов обеспечения отказоустойчивости. Основной метод повышения избыточности в распределенных ИС – репликация (дублирование данных). Если ИС реплицирована, она может продолжать работу после сбоя одной из копий просто переключившись на другую. Кроме того, поддерживая несколько копий легче противостоять сбоям данных. Когда РС масштабируется на множество машин и географических зонах, репликация повышает производительность.

При масштабировании на увеличивающуюся зону использование репликации позволяет помещать копии данных близко от использующего ее процесса, что позволяет сократить время доступа.

Проблемы, которые порождают репликации, связаны с тем, что каждый раз при изменении одной из копий необходимо провести обновление во всех остальных копиях. Скорость и частота таких обновлений влияет на стоимость всей системы и на непротиворечивость данных.

5. Безотказность - способность непрерывно работать в течение длительного времени.

Отказ системы – это такое ее поведение, которое не удовлетворяет ее спецификациям. Его причинами могут стать неверная работа каких-либо элементов, ошибки при их конструировании, программировании или производстве, физические повреждения, неверные данные и др.

Существует несколько типов отказов [7]:

а) ошибка синхронизации;

б) пропуск данных;

в) поломка.

Отказы могут быть постоянными, периодическими или случайными. Причиной случайного отказа может оказаться, например, электромагнитная помеха или редкая последовательность команд к операционной системы от нескольких процессов. Такие отказы устраняются повторным выполнением операции.

Периодические отказы могут происходить из-за плохого контакта или некорректной работы операционной системы после возникновения аварийной ситуации. Обычно они повторяются несколько раз в течение определенного интервала времени, а потом не происходят долгое время.

Постоянные или устойчивые отказы можно прекратить только при условии устранения их причины – физической поломки или ошибок в программе [8].

Для обеспечения надежности решения задач при наличии отказов, используется два принципиально разных подхода: восстановление работоспособности после отказа системы или отдельного элемента и предотвращение отказа системы – отказоустойчивость. Главным принципом отказоустойчивости является исправление ошибок после их возникновения.

Методы обеспечения надежности можно разделить на два класса. К первому относятся те, которые обеспечивают безошибочность функционирования системы, а ко второму те, которые обнаруживают ошибки и исправляют их, то есть осуществляют наблюдения за достоверностью информации и, при необходимости, ее корректировку.

Можно сказать, что обеспечение формируется при помощи совокупности факторов, которые помогают достичь необходимой цели [9]. Временное и экономическое обеспечения, которые обусловлены необходимостью, соответственно, материальных и временных затрат, нужны для осуществления действий по поддержанию достоверности. Организационное, техническое, эксплуатационное и социальное обеспечения повышают надежность систем, а структурное и алгоритмическое обеспечения – еще и достоверность информации. Анализ надежности целесообразно осуществлять на следующих этапах:

1) проектирование системы;

2) изготовление оборудования;

3) эксплуатация системы.

Проблемы надежности распределенных информационных систем можно разбить на две большие группы:

а) проблемы, связанные с надежностью программного обеспечения;

б) проблемы, связанные с надежностью аппаратуры.

Одним из перспективных путей решения проблемы надёжности программного обеспечения является реализация детально регламентированного технологического процесса [10]. При этом необходимый уровень регламентации достигается за счет структурного подхода к обеспечению надежности на различных стадиях жизни программного обеспечения.

Среди известных путей повышения надежности программного обеспечения особое внимание уделяется прогрессивным методам создания программ и широкому использованию средств автоматизации, поскольку в основе рассматриваемых методов и их инструментальной поддержки лежит структурный подход к созданию программного обеспечения. Соответствующие структурные методы оказывают большое влияние на характеристики надежности функционирования программного обеспечения. В целом структурный подход позволяет повысить эффективность работы с программным обеспечением на основе реализации трех положений: упорядочивания и унификации структурного построения программного комплекса; упорядочивания работ по устранению ошибок; создания условий для эффективного применения технологии сборочного программирования на основе программного задела.

С понятием надежности программ тесно связано понятие ошибок в программах. Результаты анализа ошибок в программах показывают, что сложное программное обеспечение не может существовать в абсолютно отлаженном состоянии. Источниками снижения надежности программ являются ошибки, вносимые в программы при проектировании, разработке и внедрении. На стадии структурного проектирования возможны ошибки в определении структуры программ.

Существует два вида распределенных алгоритмов: отказоустойчивые и стабилизирующие. Отказоустойчивые алгоритмы позволяют гарантировать правильную работу системы за счет осторожности выполнения всех шагов и тщательной проверки достоверности информации. Они используются в случаях, когда прерывание работы невозможно. Стабилизирующие алгоритмы предназначены для защиты от временных сбоев и помогают вернуть систему к работоспособному состоянию после их возникновения.

Основные проблемы надежности аппаратуры – это потенциальная ненадежность физических компонентов, их уязвимость с точки зрения безопасности и подверженность аппаратным отказам. Причиной аппаратных отказов является полная потеря работоспособности отдельно взятых элементов, вызванная каким-либо необратимым нарушением их физического состояния.

Между тем сложным ИС присущи нарушения работоспособности, которые не связаны с необратимым нарушением физического состояния элементов, входящих в её состав. Такие отказы, как сбои, т.е. кратковременные самовосстанавливающиеся отказы, характерны микропроцессорам, элементам со структурным или информационным резервированием с последующим восстановлением функционирования системы. Свойствами сбоев обладают отказы радиотехнических измерителей параметров движения объекта из-за действия помех. Нарушения работы радиотехнических, телевизионных и ультразвуковых датчиков ИС интерпретируются как постепенный отказ. Перечисленные отказы имеют одну общую особенность – при их возникновении не требуются организационные или технические меры по их устранению. Эти отказы «самоустраняются».

Надежность со стороны технических элементов может обеспечиваться за счет избыточности оборудования. Выполняемые операции дублируются, после чего результаты сравниваются для проверки правильности. Если выявлена поломка, то вышедший из строя компонент ремонтируется или заменяется на новый, пока его функции выполняются работающими аналогами.

Чтобы обеспечить надежность функционирования оборудования, обычно производится [11]:

- дублирование оборудования;
- применение проверенных протоколов работы компонентов;
- защита информации с помощью специальных технических средств.

Для того, чтобы обеспечить надежное функционирование ИС, необходимо тщательное тестирование. Для компьютеров одной из наиболее эффективных мер комплексного обеспечения надежности ИС является кластеризация и использование отказоустойчивого оборудования. В теории надежности очень важным является разделение элементов и систем на восстанавливаемые и невосстанавливаемые. Содержательный смысл этих понятий очевиден. Они помогают более обоснованно решать задачи надежности.

Ключевой подход для поддержания отказоустойчивости ИС – избыточность оборудования. Часто используют активное размножение. В качестве примера можно привести тройное дублирование аппаратуры в бортовых компьютерах.

В ходе проведенного анализа выявлены проблемы надежности распределенных информационных систем и их возможные решения, которые структурированы и представлены в виде таблицы 1.

Таблица 1 – Проблемы надежности РИС и подходы к решению

Проблемы	Подходы к решению
Связанные с надежностью программного обеспечения	
• некорректные входные данные;	• разработка методологической теории надежности программного обеспечения;

• ошибки оператора; • некорректная работа ОС; • усложнение структуры ИС.	• дублирование данных и периодическое повторение информационных процессов; • автовосстановление поврежденных средств, приложений и данных; • создание контрольных точек; • проверка достоверности информации и ее корректировка; • прогрессивные методы создания программ и привлечение средств автоматизации; • тщательное тестирование; • построение отказоустойчивых и стабилизирующих алгоритмов; • использование специальных средств для защиты информации.
Связанные с надежностью аппаратуры	
• уязвимость элементов и подверженность аппаратным отказам; • увеличение количества элементов; • неверное срабатывание элементов; • физические повреждения и износ.	• уменьшение числа компонентов; • соблюдение технических условий работы элементов; • использование стандартизированных компонентов; • кластеризация и использование отказоустойчивого оборудования; • избыточность оборудования и активное размножение; • использование стандартных протоколов работы устройств ИС.

Таким образом, с увеличением сложности систем появляется больше различных проблем, однако методы их решения также усложняются и развиваются, что позволяет поддерживать надежность на должном уровне.

Список литературы:

1. Максимов, Я. А. Технология автоматизированного моделирования надежности информационных систем // Научный электронный архив. – Режим доступа: http://econf.rae.ru/article/4574 (дата обращения: 23.12.2019).
2. Царев, Р. Ю. К проблеме оценки надежности сложных программных систем / Р. Ю. Царев, Е. Н. Штарик, А. В. Штарик // Журнал Сибирского федерального университета. Серия: Техника и технологии, 2015. – Т. 8. – № 1. – с. 33-47.

3. Таненбаум, Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен – СПб.: ПИТЕР, 2010. – 877 с.
4. Бурдонов, И. Б. Обзор подходов к верификации распределенных систем. / И. Б. Бурдонов, А. С. Косачев, В. Н. Пономаренко, В. З. Шнитман. – М.: Российская Академия Наук. Институт системного программирования (ИСП РАН), 2003. – 51 с.
5. Цветков, В. Я. Проблемы распределенных систем / В. Я. Цветков, А. Н. Алпатов – ПНиО, 2014. №6 (12).
6. Уткин, Л. В. Методы и модели анализа надежности и безопасности информационных систем при неполной информации: автореф. дис. ... д-ра техн. наук Уткина Л.В.; СПб, 2001. – 305 с.
7. Шубинский, И. Б. Структурная надежность информационных систем. Методы анализа – М.: «Журнал Надежность», 2012. – 216 с.
8. Уткин, Л. В. Нетрадиционные методы оценки надежности информационных систем. / Л. В. Уткин, И. Б. Шубинский. – СПб.: Любавич, 2000. – 173 с.
9. Демиденко, О. М. Сравнительный анализ математических методов повышения надежности информационных и технических систем / О. М. Демиденко, А. И. Кучеров. – ПФМТ, 2015, № 1 (22), с. 92-97.
10. Голоскоков, К. П. Структурный подход к повышению надежности программного обеспечения информационных систем / К. П. Голоскоков, М. Ю. Чиркова // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. – 2018. – Т. 10. – № 4 – с. 880-887.
11. Мальков, М. В. О надежности информационных систем. Труды Кольского научного центра РАН, 3 (4), с. 49-58.