ПРИНЦИПЫ ПОСТРОЕНИЯ ОТКАЗОУСТОЙЧИВЫХ ИС

I. Стороны надежности ИС

Надежность - это сложное свойство, включающее в себя более простые свойства объекта, которые называются сторонами надежности.

Сторонами надежности являются:

1. **Безотказность** - свойство объекта непрерывно сохранять работоспособность в течение некоторого времени или некоторой наработки. Наработка – время работы объекта до первого отказа.
2. **Ремонтопригодность** - свойство объекта, заключающееся в приспособленности его к предупреждению и обнаружению отказов и восстановлению работоспособности объекта либо путем проведения ремонта, либо путем замены отказавших элементов.
3. **Долговечность** - свойство объекта сохранять работоспособность до наступления предельного состояния при установленном режиме технического обслуживания и ремонта.

4. **Сохраняемость** - свойство объекта сохранять работоспособность в течение и после его хранения и (или) транспортировки.

5. **Работоспособность** - такое состояние ИС, при котором она способна выполнять заданные функции, удовлетворяя требованиям нормативно-технической документации.

6. **Живучесть** - свойство объекта или системы сохранять работоспособность (полностью или частично) в условиях неблагоприятных воздействий, не предусмотренных нормативными условиями эксплуатации.

7. **Отказоустойчивость** - свойство системы продолжать выполнение заданных функций после возникновения *сбоев* или *отказов* элементов.

8. **Конфигурация** - совокупность и способ взаимодействия программных и аппаратных средств ИС.

9. **Реконфигурация** - изменение состава и способа взаимодействия программных и аппаратных средств ИС с целью исключения отказавших элементов.

10. **Ремонт** - восстановление работоспособности системы с помощью специалистов.

II. Задачи создания отказоустойчивых ИС

При создании новых ИС стоят две противоречивые задачи:

а) достижение высокой производительности;

б) обеспечение высокой надежности.

Пути решения:

а) повышение быстродействия отдельных элементов ИС и максимальное распараллеливание процесса обработки данных.

б) возможны два основных подхода:

1. **Предотвращение отказов** путем повышения технологического уровня изготовления компонентов ИС, минимизации ошибок разработчиков, программистов, операторов.

Пути реализации:

- входной контроль,
- повышение степени интеграции элементов,
- эффективные методы рассеивания тепловой энергии.

Ограничения: естественные ограничения технического и экономического характера.

2. **Создание отказоустойчивых систем**. Допускается возникновение отказов, но используются эффективные методы устранения их последствий.

Активная отказоустойчивость базируется на процессах

- обнаружения отказа,
- локализации отказа ,
- реконфигурации системы (устраняются отказавшие элементы).

Характеризуется

(+) более экономным расходом аппаратных средств,

(-) некоторыми потерями времени при восстановлении работы системы после отказа,

(-) возможны потери некоторой части данных).

Реализуется только в многопроцессорных системах (с общей памятью, общей шиной, кольцевой, иерархической или другой структурой).

.

Пассивная отказоустойчивость заключается в способности ИС не потерять свои функциональные свойства в случае отказа отдельных элементов (отказ маскируется системой).

Характеризуется

(+) отсутствием потерь информации,

(-) увеличением объема аппаратуры в несколько раз;

Структура пассивно отказоустойчивых систем основана на

- мажоритарном принципе,
- на резервировании с контролем.

Количество резервной и дополнительной аппаратуры в таких системах превышает количество основной аппаратуры.

Применяется тогда, когда недопустимы даже кратковременные перерывы в работе ИС.

III. Обеспечение отказоустойчивости

Отказоустойчивость ИС обеспечивается введением избыточности - созданием определенных запасов или резервов.

В отказоустойчивых ИС может быть использована избыточность

- параметрическая,
- временная,
- алгоритмическая,
- структурная.

Параметрическая - облегчение режимов работы элементов и узлов аппаратуры. Малоэффективна в хорошо спроектированных ИС.

Временная - заключается в наличии дополнительного времени для решения задачи (в т.ч. для повторной обработки данных).

Создает предпосылки для реализации реконфигурации, повторения вычислений.

Алгоритмическая - заключается в применении алгоритмов, которые обеспечивают удовлетворительные результаты в случае наличия или возникновения ошибок в процессе обработки информации.

Предполагает наличие временной избыточности и является средством ее реализации.

Свойствами избыточных алгоритмов обладают итерационные алгоритмы (обеспечивают сходимость при больших случайных от клонениях промежуточных результатов).

Структурная - выражается в наличии дополнительных элементов, узлов, устройств в структуре ИС, предназначенных для автоматической замены отказавших компонентов.

Является наиболее эффективным видом избыточности.

Последовательность состояний отказоустойчивой ИС

- Работоспособное состояние ,
- Возникновение ошибки,
- Выявление ошибки,
- Локализация ошибки,
- Реконфигурация системы,
- Восстановление потерянной информации,
- Восстановление вычислительного процесса,
- Работоспособное состояние системы

Способы и средства нейтрализации ошибок и отказов в ИС

Простейший способ - повторение вычислений.

Позволяет устранить только ошибки, вызванные сбоями, и требует значительных затрат машинного времени.

На практике используют

- маскирование ошибочных действий;
- реконфигурацию системы.

Маскирование ошибочных действий - избыточная информация скрывает действие ошибочной информации за счет особенностей схемных решений и организации процесса обработки данных.

Средства маскирования делятся по принципу действия на

- корректирующие коды (CRC, Хэмминга, итеративные коды и др.);
- логика с переплетениями;
- схемы с голосованием.

Реконфигурация системы - изменение состава средств обработки информации или способа их взаимодействия.

Производится после выявления отказа.

Включает:

- статическую реконфигурацию;
- динамическую реконфигурацию.

Статическая - осуществляется путем отключения отказавших компонентов.

Система делится на две части: **активную**, участвующую в работе, и **пассивную**, охватывающую неработоспособные компоненты системы и отключенные в ходе реконфигурации.

Динамическая делится на

- реконфигурация замещением (поддержка запасом),
- р. дублированием.

На практике: DR (Dynamic Reconfiguration - динамическая реконфигурация) - способность изменять аппаратные ресурсы сервера без необходимости его закрытия, она важна в любой среде, где приоритетом является период безотказной работы прикладной программы.

Поддержка **ДР** со стороны аппаратных средств и операционной системы не достаточна.

Пока приложения не будут иметь информацию и возможность реагировать на изменения основных системных ресурсов, события ДР могут быть не в состоянии завершиться успешно.

Пример. Должна быть удалена системная плата с ЦП и памятью. Все процессы, выполняющиеся на ее ЦП, должны быть перемещены на ЦП другой системной платы, а все активные страницы должны быть перемещены в другое место памяти или выгружены на диск.

Платы устройств ввода/вывода не могут быть отсоединены от системы, если не был сконфигурирован переход на AP (Alternate Pathing - альтернативную маршрутизацию), обеспечивающую другой маршрут доступа к необходимым дискам и сетевым устройствам.

Операционная система Solaris и серверы фирмы Sun поддерживают DR.

http://ossolaris.ru/administrirovanie-ustrojstv-i-upravlenie-diskami/vypolnenie-zapuska-sistemy-s-rekonfiguraciej.html

Подробно описан процесс выполнения запуска системы с реконфигурацией.

Пример. Sun Fire E25k (кодовое имя *«Amazon 25»*) — высокопроизводительный сервер уровня предприятия от корпорации **Sun Microsystems**

Некоторые параметры:

Межкомпонентное соединение : продублированный коммутатор 18x18 для данных и адресов,

Ввод/вывод : До 72 слотов ввода/вывода PCI на 18 каналах с возможностью «горячей замены»;

Системный контроллер : 2 дублированных системных контроллера. Автоматическая система восстановления системных контроллеров после сбоя, автоматическое восстановление функций управления и часов системных контроллеров, без необходимости остановки операций ;

Готовность : Полное дублирование аппаратного обеспечения

- «Горячая замена» процессоров
- Модернизация в режиме он-лайн
- Журналирование файловой системы
- Сервисное обслуживание без остановки процессов вычислений
- ECC-защита на всех уровнях
- Резервные сетевые соединения
- Резервные соединения систем хранения данных
- Стабильное ядро ОС
- Высоконадежные драйверы ввода/вывода

Способы восстановления отказоустойчивой ИС

После реконфигурации для продолжения нормальной работы ИС необходимо ее восстановить.

Восстановление системы происходит на двух уровнях :

1. **Аппаратный уровень**.

Для восстановления используют два способа:

- *Автоматическое* в. - путем дополнительной реконфигурации (в системе имеется ряд запасных блоков);
- *Ремонт* (восстановление вручную).

2. **Программный уровень**.

Способы восстановления:

- *повторение операции* на различных уровнях (команд или микрокоманд);

повторное выполнение может дать правильный результат, если связанная с ними ошибка является случайной или временной (ошибка исчезает в процессе восстановления);

- *возвращение к контрольной точке*.

Контрольная точка - некоторый этап процесса обработки информации, для которого зафиксированы (в ЗУ) промежуточные результаты и информация о состоянии системы, позволяющая возобновить обработку данных.

При обнаружении ошибки система возвращается к КТ, предшествующей моменту возникновения отказа, и продолжает работу, используя данную точку в качестве исходной;

- *повторное выполнение программы*.

Все незавершенные (до возникновения отказа) программы выполняются с самого начала. Применяется в случаях:

а) если последствия отказа успели отразиться на большей части системы;

б) если возможно восстановление только части вычислительных процессов;

в) если продолжение работы системы при использовании других способов восстановления сопряжено с трудностями и большими затратами времени.

Испытания ИС на надежность

Испытания на надежность - это определение показателей надежности объекта на основании непрерывного наблюдения за состоянием его работоспособности в условиях, предписанных методикой испытаний.

Испытания на надежность являются обязательным видом испытаний при изготовлении изделий и при приемке их от заводов-изготовителей.

Методики проведения таких испытаний регламентируются Государственными и отраслевыми стандартами.

- **ГОСТ 27.002-89 МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ НАДЕЖНОСТЬ В ТЕХНИКЕ** Основные понятия. Термины и определения
- **ГОСТ Р 27.403-2009** Надежность в технике. Планы испытаний для контроля вероятности безотказной работы

- **Другие ГОСТы**
- ГОСТ Р МЭК 60605-6-2007 Надежность в технике. Критерии проверки постоянства интенсивности отказов и параметра потока отказов
  ГОСТ 17331-71 Надежность в технике. Метод последовательных испытаний
  ГОСТ 27.410-87 Надежность в технике. Методы контроля показателей надежности и планы контрольных испытаний на надежность
  ГОСТ Р МЭК 61650-2007 Надежность в технике. Методы сравнения постоянных интенсивностей отказов и параметров потока отказов
  ГОСТ Р 27.004-2009 Надежность в технике. Модели отказов
  ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения
  ГОСТ Р 53480-2009 Надежность в технике. Термины и определения
  ГОСТ 27.003-90 Надежность в технике. Состав и общие правила задания требований по надежности
  ГОСТ 27.004-85 Надежность в технике. Системы технологические. Термины и определения
  ГОСТ Р 27.001-2009 Надежность в технике. Система управления надежностью. Основные положения
  ГОСТ 27.301-95 Надежность в технике. Расчет надежности. Основные положения
  ГОСТ Р 27.404-2009 Надежность в технике. Планы испытаний для контроля коэффициента готовности

Особенности надежностных испытаний ИС

1. **Исключение «анормальных» результатов испытаний**.

- Статистические данные о надежности элементов системы, собираются на разных объектах.
- Важно обеспечить однородность статистического материала.
- «Аномальные» результаты испытаний должны исключаться

из статистической совокупности по правилам :

1) если некоторое измерение $x_к$ (из **N**) внушает сомнение в его принадлежности к генеральной совокупности, то определяются:

а) среднее значение $x_{ср}$ и среднеквадратическое отклонение σ генеральной совокупности без сомнительных измерений;

б) коэффициент **k**: $k = (x_к - x_{ср})/ \sigma,$

где

$$\sigma = \sqrt{\sum (x_i - x_{ср})^2 / (N-1)}$$

- 2) если **k** больше допустимого значения, указанного в специальной таблице допустимых значений, то делается вывод о том, что $\mathbf{x_к}$ не принадлежит к генеральной совокупности.

Пример.

Определить наличие “анормальных” измерений, если получены измерения (N=17):

1. 0,9986	5. 0,9996	10. 0,9975	14. 0,9993
2. 0,9997	6. 0,9759	11. 0,9997	15. 0,9995
3. 0,9934	7. 0,9986	12. 0,9998	16. 0,9996
4. 0,9991	8. 0,9986	13. 0,9998	17. 0,9992
9. 0,9993			

При использовании таблицы значений допустимых **k**:

Число измерений	4	6	8	10	12	14	16
Значение k	1,49	1,94	2,22	2,41	2,55	2,66	2,75

Предварительный анализ состава измерений ставит под сомнение результаты **3, 6**, как существенно отличающиеся от остальных.

Произведем обработку основной группы измерений:

$$X_{ср} = \sum X_i/15 = 0{,}999$$ (здесь N=15)

$$\sigma = \sqrt{\sum (x_i - x_{ср})^2 / (N-1)} = 0{,}0008$$

$$k = 7.$$

Определим по приведенной выше таблице предельно допустимое значение **k** для 15 измерений. Оно не превышает **2,75**.

Следовательно, полученное значение k для 3 и 6измерений значительно больше допустимого значения, поэтому результат третьего и шестого измерений – «анормальный».

2. **Использование ускоренных испытаний.**

Испытания при повышенных температурах, влажности, токах, напряжениях и т.д.

Для этого д.б. известны соотв. зависимости и влияния

- **Наиболее целесообразным решением проблемы оценки надежности ИС в целом является расчетно-экспериментальный метод, т.е. сочетание натурных испытаний и расчетов, и последующее подтверждение полученных расчетных оценок с помощью ограниченного объема испытаний.**

•Каждая большая система требует разработки своей методики испытаний, отражающей ее особенности. Испытания элементов, входящих в состав большой системы, следует рассматривать в качестве предварительного этапа испытаний всей системы.