ИНФОРМАТИКА

2008 **январь-март** **№ 1**

ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ СИСТЕМ

УДК 004.3

В.В. Анищенко, Л.И. Кульбак, Т.С. Мартинович

АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ПОДДЕРЖКИ НАДЕЖНОСТИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Рассматриваются способы и методы аппаратно-программной поддержки надежности технических средств (ТС) информационно-вычислительных систем. Приводятся формулы расчета показателей надежности ТС и группы зарезервированных ТС с учетом полноты контроля их состояния в процессе работы и полноты сохранения информации, предшествующей их отказу.

Введение

Надежность информационно-вычислительных систем (ИВС) в значительной степени зависит от надежности составляющих их компонентов. Компонентами ИВС являются ТС и их программное обеспечение (ПО). К ТС ИВС относятся: компьютеры (рабочие станции или автоматизированные рабочие места), сетевые устройства в виде серверов (файловых, баз данных, приложений, электронной почты, веб-серверов и др.), средства коммуникаций (коммутаторы, маршрутизаторы, мосты, шлюзы и др.), сетевые каналы связи между ТС. Заметим, что в настоящее время роль мостов и шлюзов успешно выполняют маршрутизаторы.

Программные средства поддержки надежности ИВС содержатся как в операционных системах (ОС) ТС, так и в прикладных (пользовательских) программах клиентов ИВС. В качестве ОС ИВС ограничимся рассмотрением семейства Windows 2000 (Windows Professional, Windows Server, Advanced Server, Datacenter Server) и совместимых с ним программ.

ИВС, как правило, является многофункциональной системой, которую можно разделить на отдельные функциональные подсистемы (ФП). Согласно нормативной документации [1] требования к надежности многофункциональных систем заменяются требованиями к надежности ФП. При этом в качестве показателя надежности непрерывно работающих ФП рекомендуется использовать коэффициент готовности K_{Γ}.

В зарубежных технических источниках коэффициент готовности часто трактуется как показатель доступности к системе и выражается в процентах. При этом в качестве показателя надежности ФП стали часто использовать среднее время ее вынужденного простоя в течение календарного года при условии круглосуточной работы без перерыва на техническое обслуживание [2]. Этот показатель можно вычислить по формуле

$$T_{\text{СР.Г}} = 8760\,(1 - K_{\Gamma}),$$

где $T_{\text{СР.Г}}$ – среднее время вынужденного простоя ФП в течение календарного года; 8760 – количество часов в году; K_{Γ} – коэффициент готовности ФП.

1. Формулы оценки показателей надежности ТС ИВС

Особенность ТС ИВС состоит в том, что их отказы сразу могут не проявляться и ТС может продолжать работу в состоянии скрытого отказа, неправильно выполняя заданную работу. Даже при своевременном обнаружении отказа информация на момент, предшествующий отказу, может не сохраниться, и при восстановлении работоспособности ТС сможет продолжить начатую работу только после восстановления информации, имевшейся на момент отказа. Часто восстановление этой информации производится повторным выполнением задания. В этом случае теряется время, которое было израсходовано к моменту возникновения отказа, поэтому

восстановление работоспособности ТС еще не означает восстановление прерванного вычислительного процесса.

Получим формулы оценки коэффициента готовности одиночного ТС и группы зарезервированных ТС с учетом полноты контроля их состояния и восстановления потерянной информации. Для вывода формул воспользуемся методами, приведенными в работе [3].

1.1. Одиночное (незарезервированное) ТС

Незарезервированное ТС в процессе его эксплуатации можно представить размеченным графом (рис. 1), на котором определены его следующие состояния: 0 – ТС выполняет назначенную работу (рабочее состояние); 1 – произошел отказ ТС и он обнаружен (выявленное нерабочее состояние); 2 – отказ ТС не обнаружен (скрытый отказ); 3 – работоспособность ТС восстановлена, но информация, необходимая для продолжения работы, не сохранена; 4 – обнаружен скрытый отказ ТС; 5 – работоспособность ТС восстановлена и сохранена информация, предшествующая скрытому отказу, но не восстановлена информация, которая могла иметься к моменту обнаружения скрытого отказа; 6 – работоспособность ТС восстановлена, но не сохранена информация, предшествующая скрытому отказу, и не восстановлена информация, которая могла иметься к моменту обнаружения скрытого отказа.

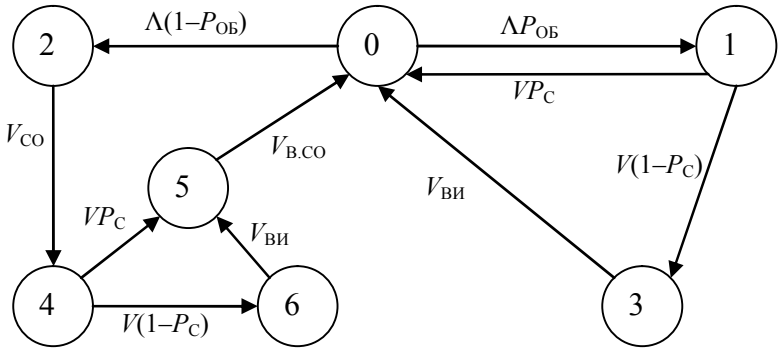

Рис. 1. Граф состояний незарезервированного ТС: Λ – интенсивность отказов ТС; $P_{ОБ}$ – полнота контроля состояния ТС (вероятность определения потери работоспособности ТС); P_C – вероятность сохранения после отказа ТС информации, необходимой для продолжения работы; V – интенсивность восстановления работоспособности ТС; V_{CO} – интенсивность выхода ТС из состояния скрытого отказа; $V_{ВИ}$ – интенсивность восстановления информации, необходимой для продолжения работы и потерянной ввиду отказа; $V_{В.СО}$ – интенсивность восстановления информации, необходимой для продолжения работы и потерянной ввиду скрытого отказа ТС

В работе [3] показано, что коэффициент готовности ТС в рассматриваемом случае определяется по формуле

$$K_Г = P_0 ,$$

где P_0 – вероятность пребывания ТС в состоянии «0».

Вероятность P_0 определяется из системы уравнений

$$\begin{cases} V P_1 = \Lambda P_{ОБ} P_0; \\ V_{CO} P_2 = \Lambda (1–P_{ОБ}) P_0; \\ V_{ВИ} P_3 = V (1–P_C) P_1; \\ V P_4 = V_{CO} P_2; \\ V_{В.СО} P_5 = V P_C P_4 + V_{ВИ} P_6; \\ V_{ВИ} P_6 = V (1–P_C) P_4; \\ \sum_{i=0}^{6} P_i = 1, \end{cases} \quad (1)$$

где P_1, …, P_6 – вероятности пребывания системы в состояниях 1, …, 6 соответственно.

В результате решения системы уравнений (1) получено

$$K_{\Г} = \frac{T_{\О}}{T_{\О} + T_{\В} + (T_{\СО} + T_{\В.\СО})(1 - P_{\ОБ}) + T_{\ВИ}(1 - P_{\С})}, \quad (2)$$

где $T_{\О}$ – средняя наработка на отказ ТС; $T_{\В}$ – среднее время восстановления аппаратной части ТС; $T_{\СО}$ – среднее время пребывания ТС в состоянии скрытого отказа; $T_{\ВИ}$ – среднее время восстановления информации, необходимой для продолжения работы и потерянной ввиду отказа; $T_{\В.\СО}$ – среднее время восстановления информации, необходимой для продолжения работы и потерянной ввиду скрытого отказа ТС. При этом $T_{\О} = 1/\Lambda$, $T_{\В} = 1/V$, $T_{\СО} = 1/V_{\СО}$, $T_{\ВИ} = 1/V_{\ВИ}$, $T_{\В.\СО} = 1/V_{\В.\СО}$.

Из формулы (2) следует, что коэффициент готовности ТС $K_{\Г}$ зависит от средней наработки на отказ ТС (безотказности ТС); среднего времени восстановления ТС $T_{\В}$ (ремонтопригодности ТС); полноты контроля состояния ТС $P_{\ОБ}$; периодичности достоверного контроля состояния ТС (среднего времени пребывания ТС в состоянии скрытого отказа $T_{\СО}$); вероятности сохранения информации, непосредственно предшествующей отказу ТС $P_{\С}$; среднего времени, расходуемого на восстановление информации до уровня, предшествующего обнаруженному отказу ТС $T_{\ВИ}$ и скрытому отказу $T_{\В.\СО}$. Из формулы (2) также следует, что при полном контроле состояния ТС ($P_{\ОБ} = 1$) и полном сохранении информации, предшествующей отказу ТС ($P_{\С} = 1$), коэффициент готовности достигает максимального значения и равняется коэффициенту готовности аппаратной части ТС.

Таким образом, все средства, которые способствуют сокращению числа отказов ТС, времени восстановления аппаратной части ТС, интервала между моментом сохранения информации, предшествующей отказу, и моментом наступления отказа, а также повышению полноты контроля состояния ТС, частоты достоверного контроля состояния ТС, вероятности сохранения информации, предшествующей отказу ТС, позволяют повысить надежность одиночного (незарезервированного) ТС.

1.2. Зарезервированное ТС

Рассмотрим два ТС, которые работают одновременно над выполнением одного задания. В процессе работы ТС обмениваются информацией, которая способствует своевременному обнаружению отказа одного из ТС. При отказе одного из ТС работа продолжается оставшимся работоспособным ТС, а отказавшее ТС подвергается восстановлению. При отказе второго ТС наступает отказ зарезервированной системы и ее восстановление производится ускоренным методом. Если работает одно ТС, полнота контроля его состояния становится отличной от единицы.

Состояния группы зарезервированных ТС в процессе их эксплуатации можно представить размеченным графом (рис. 2): 0 – оба ТС работоспособны; 1 – отказало одно ТС, отказ обнаружен и работу продолжает второе ТС; 2 – восстановлена аппаратная часть отказавшего ТС, но информация, позволяющая поддержать работу второго ТС, не восстановлена; 3 – неработоспособны оба ТС, что было обнаружено; 4 – отказало второе ТС, которое продолжало работу, но отказ не был обнаружен (состояние скрытого отказа); 5 – обнаружен отказ второго ТС (выход из состояния скрытого отказа); 6 – восстановлена аппаратная часть второго ТС; 7 – восстановлена аппаратная часть второго ТС в случае обнаружения его отказа.

В соответствии с методологией [3] коэффициент готовности группы ТС в рассматриваемом случае определяется по формуле

$$K_{\Г} = P_0 + P_1,$$

где P_0 – вероятность пребывания группы ТС в состоянии «0»; P_1 – вероятность пребывания группы ТС в состоянии «1».

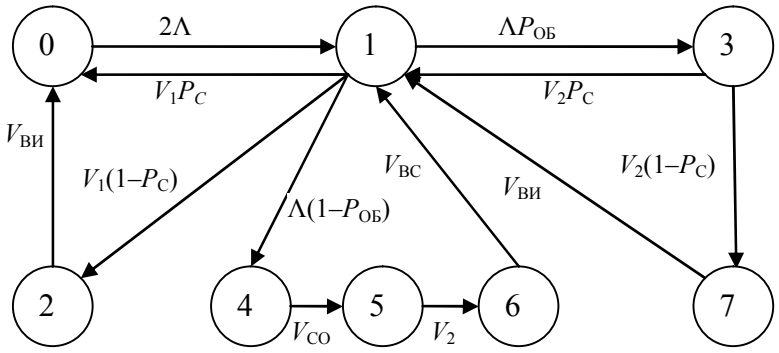

Рис. 2. Граф состояний группы зарезервированных ТС: Λ – интенсивность отказов ТС; $P_{\text{ОБ}}$ – вероятность определения потери работоспособности одиночного ТС; $P_{\text{С}}$ – вероятность сохранения информации, необходимой для продолжения работы, в случае отказа ТС; V_1 – интенсивность восстановления работоспособности ТС, которое отказало первым; V_2 – интенсивность восстановления работоспособности одного из двух ТС в случае, когда отказали оба ТС; $V_{\text{ВИ}}$ – интенсивность восстановления информации, необходимой для продолжения работы, в случае, когда отказ был обнаружен; $V_{\text{ВС}}$ – интенсивность восстановления информации, необходимой для продолжения работы, в случае, когда обнаружен скрытый отказ; $V_{\text{СО}}$ – интенсивность обнаружения скрытого отказа (интенсивность достоверного контроля ТС)

Вероятности P_0 и P_1 определяются из системы уравнений

$$\begin{cases} 2\Lambda P_0 = V_1 P_{\text{С}} P_1 + V_{\text{ВИ}} P_2; \\ V_{\text{ВИ}} P_2 = V_1 (1-P_{\text{С}}) P_1; \\ V_2 P_3 = \Lambda P_{\text{ОБ}} P_1; \\ V_{\text{СО}} P_4 = \Lambda(1-P_{\text{ОБ}}) P_1; \\ V_2 P_5 = V_{\text{СО}} P_4; \\ V_{\text{ВС}} P_6 = V_2 P_5; \\ V_{\text{ВИ}} P_7 = V_2 (1-P_{\text{С}}) P_3; \\ \sum_{i=0}^{7} P_i = 1. \end{cases} \qquad (3)$$

В результате решения системы уравнений (3) получим

$$K_{\Gamma} = \frac{T_{\text{О}} + 2T_{\text{В.1}}}{T_{\text{О}} + 2T_{\text{В.1}} + \frac{2}{T_{\text{О}}}[T_{\text{В.1}} T_{\text{В.2}} + T_{\text{ВИ}}(1-P_{\text{С}})(T_{\text{О}} + T_{\text{В.1}} P_{\text{ОБ}}) + T_{\text{В.1}}(1-P_{\text{ОБ}})(T_{\text{СО}} + T_{\text{ВС}})]}, \qquad (4)$$

где $T_{\text{О}}$ – средняя наработка на отказ ТС; $T_{\text{В.1}}$ – среднее время восстановления ТС, которое отказало первым; $T_{\text{В.2}}$ – среднее время восстановления одного из двух отказавших ТС; $T_{\text{ВИ}}$ – среднее время восстановления информации, необходимой для продолжения работы в случае, когда отказ был обнаружен; $T_{\text{СО}}$ – среднее время пребывания ТС в состоянии скрытого отказа; $T_{\text{ВС}}$ – среднее время восстановления информации, необходимой для продолжения работы в случае, когда обнаружен скрытый отказ. При этом $T_{\text{В.1}} = 1/V_1$; $T_{\text{В.2}} = 1/V_2$; $T_{\text{ВИ}} = 1/V_{\text{ВИ}}$; $T_{\text{СО}} = 1/V_{\text{СО}}$; $T_{\text{ВС}} = 1/V_{\text{ВС}}$.

Из формулы (4) следует, что коэффициент готовности зарезервированной группы ТС зависит от следующих показателей: средней наработки на отказ $T_{\text{О}}$; среднего времени восстановления первого отказавшего ТС $T_{\text{В.1}}$ и одного из двух отказавших ТС $T_{\text{В.2}}$; вероятности определения потери работоспособности одиночного ТС $P_{\text{ОБ}}$; вероятности сохранения информации, необходимой для продолжения работы, в случае отказа ТС $P_{\text{С}}$; среднего времени восстановления информации, необходимой для продолжения работы, в случае обнаружения отказа $T_{\text{ВИ}}$; среднего времени восстановления информации, необходимой для продолжения работы, в случае обнаружения скрытого отказа $T_{\text{ВС}}$; среднего времени обнаружения скрытого отказа $T_{\text{СО}}$. Из формулы (4)

также следует, что коэффициент готовности достигает максимального значения при достоверном контроле работоспособности ТС ($P_{\text{ОБ}} = 1$) и полном сохранении информации, предшествующей отказу ($P_{\text{С}} = 1$). При этом

$$K_{\text{Г.МАХ}} = \frac{T_{\text{О}} + 2T_{\text{В.1}}}{T_{\text{О}} + 2T_{\text{В.1}} + \frac{2}{T_{\text{О}}} T_{\text{В.1}} T_{\text{В.2}}} \approx 1 - \frac{2T_{\text{В.2}}}{T_{\text{О}}(2 + T_{\text{О}}/T_{\text{В.1}})}.$$

2. Распределение отказов ТС ИВС

Отказы ТС ИВС по своим проявлениям разделяются на устойчивые и неустойчивые (сбои). Устойчивые отказы устраняются лишь путем замены отказавшего элемента. Неустойчивые отказы имеют свойство проявляться не всегда, особенно после перезапуска или перезагрузки.

По данным компании Hewlett-Packard, отказы серверов связаны со следующими причинами [4]: сбой (зависание) сетевой ОС – 79 %, отказы дисковых накопителей – 5 %, отказ оперативной памяти – 4 %, проблемы сети электропитания – 8 %, отказ источника питания – 2 %, отказ центрального процессора – 1 %, другие причины – 1 %. Такое распределение отказов можно распространить и на компьютеры.

Наиболее вероятной причиной зависания ОС является появление ошибки в структуре хранения или передачи данных ОС в результате сбоя в аппаратной части ТС. Поэтому зависание ОС нейтрализуется путем перезапуска или перезагрузки ОС. Остальные отказы являются устойчивыми и нейтрализуются путем замены отказавшего элемента. Если из распределения отказов ТС убрать зависание ОС, то распределение устойчивых отказов будет следующим: отказы дисковых накопителей – 23,8 %, отказ оперативной памяти – 19,0 %, проблемы сети электропитания – 38,1 %, отказ источников питания – 9,5 %, отказ центрального процессора – 4,8 %, другие причины – 4,8 %. Из распределения отказов ТС следует, что основное внимание следует уделять системе электропитания, затем дисковой подсистеме и оперативной памяти.

В работе [5] приведена следующая статистика отказов в системах обработки данных: отказы дисковых подсистем – 28 %, отказы сервера или его ядра – 23 %, отказы из-за ошибок в программном обеспечении – 22 %, отказы коммуникационного оборудования – 15 %, отказы из-за сбоев в коммуникационных каналах передачи данных – 6 %, отказы из-за ошибок персонала – 6 %.

Приведенные статистические данные по отказам серверов и компонентов систем обработки данных целесообразно учитывать при разработке мероприятий по повышению надежности ИВС.

3. Аппаратно-программные средства обеспечения надежности компьютеров

Аппаратную структуру компьютера можно представить состоящей из следующих компонентов: системы электропитания, материнской платы, на которой размещены микропроцессор и оперативная память, системы шин связи между компонентами, подсистемы жестких дисков, параллельных и последовательных портов, порта устройств USB с клавиатурой, подсистемы гибких дисков, сетевого адаптера, видеокарты и монитора. Программное обеспечение компьютера состоит из операционной системы и приложений. Очевидно, что надежность компьютера зависит от надежности его аппаратных и программных компонентов и используемых аппаратных и программных средств обеспечения надежности. Рассмотрим возможности обеспечения надежности компонентов компьютера.

Систему электропитания компьютера можно представить в виде двух частей: системы первичного сетевого электропитания и системы вторичного электропитания. В систему первичного электропитания входит источник бесперебойного питания (ИБП), который предназначен для стабилизации сетевого напряжения и временного обеспечения электропитанием в случае отключения сетевого питания. В систему вторичного электропитания входят преобразователи переменного сетевого напряжения в постоянные напряжения тех номиналов, которые необходимы для компьютера.

ИБП защищает компьютер от сетевых помех в виде высоковольтных выбросов, падения напряжения, спадов и подъемов напряжения, нестабильности частоты, отключения напряжения

и др. В случае отказа ИБП с помощью байпаса переключает вторичные источники на питание непосредственно от сети и тем самым маскирует свой отказ. Как правило, можно производить замену ИБП, не прерывая работы компьютера, также возможна параллельная работа нескольких ИБП. Они являются надежными устройствами; например, средняя наработка на отказ ИБП UPStation GXT достигает миллиона часов [6].

Сетевые источники вторичного электропитания (ИВЭ) компьютеров имеют недостаточно высокие показатели надежности; например, ИВЭ фирмы Portwell PW-250 [7] имеет среднюю наработку на отказ 50 000 ч. Для повышения надежности системы вторичного электропитания используется нагрузочный резерв. Берется определенное количество ИВЭ, которые обеспечивают необходимую мощность потребления, и добавляется один резервный. Все ИВЭ работают параллельно, при этом отказавший ИВЭ блокируется. При возможности «горячей замены» (замены, не прерывающей работы компьютера) такая система становится отказоустойчивой.

В ядре ОС Windows 2000 имеется диспетчер управления питанием, который работает как основное звено управления событиями и сообщениями, связанными с электропитанием. Диспетчер управления питанием выполняет наблюдение за состоянием батарей ИБП, запуск, остановку и приостановку аппаратных ресурсов сбережения энергии, управление функциональностью ОС при работе в режиме с пониженным потреблением или резервной системой электропитания [8].

Для поддержания надежности работы всех компонентов, в том числе и системы электропитания, в ОС Windows 2000 Professional имеется служба Plug and Play, которая представляет собой набор драйверов устройств, позволяющий ОС управлять оборудованием компьютера, заново конфигурировать выделение ресурсов устройствам и управлять питанием. Вместе с драйверами устройств, поддерживающих управление питанием, это позволяет выполнять горячую замену многих периферийных устройств (добавление и удаление из системы без выключения компьютера) [8].

В *подсистему жестких дисков* входят контроллер жестких дисков, жесткие диски и программные средства ОС, поддерживающие работу подсистемы, в том числе и драйвер контроллера.

Контроллер жестких дисков удовлетворяет требованиям по надежности к компьютерам PC. Например, средняя наработка на отказ контроллера жестких дисков фирмы Octagon Systems 5815 [9] составляет 71 524 ч.

Накопитель на жестком диске (НЖД) является наиболее нагруженным и важным элементом компьютера. Это единственный компонент, который не подлежит эквивалентной замене, потому что на нем имеются индивидуальные файлы данных. Приведенные обстоятельства обусловливают повышенные требования к надежности дисковой подсистемы. С точки зрения устойчивых отказов НЖД является достаточно надежным элементом, например НЖД фирмы Western Digital WDE18300/AV имеет среднюю наработку на отказ порядка миллиона часов. Сведения по сбоям в характеристиках НЖД отсутствуют. Следует ожидать, что его средняя наработка на сбой значительно ниже, чем средняя наработка на отказ.

С целью повышения надежности и устойчивости к сбоям одиночных НЖД используют избыточное кодирование данных, в частности коды Хэмминга (Hamming Code ECC), которые исправляют одиночные ошибки и обнаруживают двойные.

Для исправления двойных и больших размеров ошибок следует применять зеркалирование дисков. В простейшем варианте используются два диска, на которые записывается одинаковая информация, и в случае отказа одного их них остается его дубль, который продолжает работать в прежнем режиме. Зеркалирование томов и дисков поддерживается ОС Windows 2000.

Оперативная память конструктивно представляет собой набор модулей памяти SIMM или DIMM, устанавливаемых в разъемы материнской платы. Для обеспечения надежности (предотвращения ошибок) используется контроль на четность – добавляется один контрольный разряд в каждый байт или четыре контрольных разряда на четыре байта [10]. Контроль на четность обнаруживает лишь однобитовые ошибки и не может их устранить.

Более радикальным средством повышения надежности памяти является использование модулей памяти с контролем и коррекцией ошибок (ECC – Error Checking and Correction). Память ECC, в отличие от обычной памяти с контролем на четность, позволяет обнаруживать и исправлять

ошибки в нескольких битах. При этом обнаружение и исправление ошибки не приводят к остановке работы компьютера, как это происходит в случае использования обычной памяти [4].

Система шин связи с компонентами компьютера. Согласно работе [8] у современных компьютеров имеются шины PCI, ISA, мост перехода PCI/ISA, AGP. Надежность в шинах поддерживается контролем передаваемых по ним данных на четность.

Адаптеры и порты компьютера. Средняя наработка на отказ современных компьютеров составляет порядка 15 000 – 20 000 ч (1,7 – 2,3 года). Если один из компонентов компьютера имеет среднюю наработку на отказ на порядок большую, чем сам компьютер, то можно утверждать, что она удовлетворяет требованиям по надежности к компьютеру. В качестве примера рассмотрим таблицу средней наработки на отказ компонентов компьютера фирмы Octagon Systems [9].

Таблица

Компоненты компьютера	Обозначение	Средняя наработка на отказ, ч/лет
Сетевой адаптер	5500	337 224 / 44,2
Видеоадаптер	2430	340 332 / 38,9
Плата последовательного интерфейса	5554	754 242 / 86,1
Многофункциональная плата ввода/вывода с параллельным портом и портом клавиатуры	5540	743 698 / 84,9

Из таблицы следует, что сетевой адаптер, видеоадаптер (видеокарта), последовательный и параллельный порты и порт устройств USB удовлетворяют требованиям по надежности к современным компьютерам.

Контроль работоспособности компьютера. Контроль работоспособности компьютера проводится при включении электропитания встроенной в него программой BIOS. Если работоспособность компьютера подтверждается, то происходит загрузка ОС, которая в последующем принимает на себя контроль (мониторинг) компьютера в процессе его работы.

4. Аппаратно-программные средства обеспечения надежности серверов

Структура серверов мало чем отличается от структуры компьютера, но компоненты структуры отличаются существенно как производительностью, так и потребляемой мощностью. Значение серверов в ИВС велико, и при отказе сервера ряд функций (возможно, и все) ИВС не сумеет выполнить. Отказ сервера приводит к большим материальным потерям, иногда исчисляемым в сотнях долларов. По этой причине надежности серверов уделяется пристальное внимание.

4.1. Требования по надежности, предъявляемые к серверам

Надежность серверов принято оценивать коэффициентом готовности (в зарубежных источниках его называют доступностью) K_{Γ}. В ФП ИВС могут входить несколько серверов, коммутаторы, маршрутизаторы и другие компоненты. Коэффициент готовности ФП ИВС выражается через коэффициенты готовности ее компонент следующей формулой:

$$K_{\Gamma.\Phi\Pi} = \prod_{S=1}^{M} K_{\Gamma.S} , \qquad (5)$$

где $K_{\Gamma.\Phi\Pi}$ – коэффициент готовности ФП ИВС; $K_{\Gamma.S}$ – коэффициент готовности s-й компоненты ФП ИВС; M – число компонентов в ФП ИВС.

Из формулы (5) следует, что для сервера требования по надежности должны вычисляться исходя из требований к ФП ИВС. Если предъявлять одинаковые требования по надежности ко всем компонентам ФП ИВС, то требования по надежности сервера определятся как корень s-й степени из требуемого значения $K_{\Gamma.\Phi\Pi}$. Учитывая, что значения $K_{\Gamma.\Phi\Pi}$ и $K_{\Gamma.S}$ близки к единице, требования к надежности сервера можно определить по формуле

$$K_{\Gamma.C} \approx 1 - \frac{1 - K_{\Gamma.\Phi\Pi}}{M} , \qquad (6)$$

где $K_{\Gamma.C}$ – требуемое значение коэффициента готовности сервера.

В зарубежных источниках ФП ИВС по надежности разделяют на две категории: высокодоступные и отказоустойчивые системы [2]. К высокодоступным системам в [2] отнесены системы, у которых коэффициент готовности лежит в пределах 99,5–99,9 %, к отказоустойчивым – системы, коэффициент готовности которых выше 99,9 %. Например, в работе [12] к отказоустойчивым отнесены системы, имеющие коэффициент готовности в пределах 99,900–99,999 %. Не придерживаясь такого разделения, отнесем к высоконадежным системам такие, которые обладают свойством отказоустойчивости, под которой будем понимать способность системы продолжать функционирование в случае отказа ее компонентов.

Допустим, что ФП ИВС состоит из пяти компонентов и должна иметь коэффициент готовности высоконадежной системы (не менее 0,9990). Тогда согласно формуле (6) к высоконадежным следует отнести сервер с коэффициентом готовности не менее 0,9998. Такие требования к надежности можно удовлетворить только с помощью раздельного резервирования компонентов серверов или их общего резервирования.

4.2. Обеспечение надежности раздельным резервированием компонентов серверов

В разд. 2 приведено распределение отказов серверов, из которого можно сделать вывод о необходимости в первую очередь нейтрализовать зависание ОС. Эта проблема решается аппаратно-программными средствами автоматического перезапуска сервера.

Проблемы первичного электропитания серверов решаются с помощью использования ИПБ с байпасом и их резервирования, при котором активное участие принимают программные средства (например, диспетчеры управления питанием в Windows 2000).

Для обеспечения надежности дисковой подсистемы возможны несколько вариантов. Один из вариантов – это применение двух SCSI-адаптеров, что позволяет организовать на аппаратном уровне зеркальное дублирование как дисков, так и дисковых адаптеров. Более радикальным вариантом является использование системы дисковой памяти RAID, которое представляет собой программно-аппаратные средства повышения надежности хранения данных за счет избыточности их объема. Множество физических дисков преобразуется в один логический диск, в зависимости от способа резервирования устанавливаются уровни RAID [11].

Windows 2000 поддерживает программный RAID. В программном RAID ОС выполняет все функции аппаратного RAID и системе не требуется отдельная карта контроллера для RAID, однако программный RAID менее надежен, чем аппаратный, и проигрывает ему в быстродействии [12].

Надежность дисковых подсистем можно увеличить за счет горячей замены отказавших дисков путем использования специальных отсеков для сменных дисков или автоматического перехода на встроенный запасной диск. При замене диска данные на нем подлежат восстановлению в фоновом режиме работы.

В серверах требуется большой объем памяти, что приводит к необходимости делить оперативную память на банки и использовать модули памяти с коррекцией ошибок. В этом случае все ошибки обнаруживаются, а ошибки в несколько бит исправляются. Если исправление ошибки невозможно, часть банка памяти или весь банк будут заблокированы и автоматически произойдет перезапуск системы для работы с оперативной памятью меньшего объема [4].

В настоящее время распространены многопроцессорные материнские платы, которые используются в серверах. Современные сетевые ОС поддерживают многопроцессорную обработку данных. В случае отказа микропроцессора происходит перезагрузка сервера, во время которой все процессоры тестируются и отказавшие автоматически блокируются.

Высоконадежный (отказоустойчивый) сервер имеет избыточные компоненты для каждой подсистемы. Он оснащается двумя процессорными платами (в каждой по два процессора), двумя платами памяти, двумя подсистемами ввода-вывода, несколькими сетевыми платами, зеркальными дисковыми системами с двумя главными адаптерами и несколькими точками подключения, двумя источниками питания с охлаждающими вентиляторами, двумя ИБП с идущими к разным источникам первичного питания шнурами. Все системы сервера работают в жестком параллельном режиме, и две копии ОС выполняются одновременно цикл за циклом. В случае отказа одного компонента или целой системы сервер будет продолжать выполнять свои функции [2]. Такие серверы имеют коэффициент готовности порядка 99,9995% [12].

4.3. Обеспечение надежности серверов общим резервированием

Сетевые ОС поддерживают общее резервирование серверов по нескольким технологиям SQL Server 2000, среди которых отказоустойчивая кластеризация, перемещение журналов и репликация.

Отказоустойчивая кластеризация. Кластерные технологии позволяют объединить несколько серверов для обеспечения высокого уровня надежности. Как правило, кластеры состоят из двух узлов и разделяемого (совместно используемого) дискового пространства [13]. Кластеры могут поддерживать передачу управления ресурсами при сбое, возвращение управления ресурсами на исходный узел после его восстановления, перераспределение нагрузки (ресурсов) между узлами.

Обнаружение и предотвращение отказов – главное преимущество, предоставляемое службой кластеров ОС Windows 2000 Server [14]. Когда в кластере отказывает узел или приложение, служба кластеров перезапускает отказавшее приложение или перераспределяет нагрузку отказавшей системы на работающий узел.

В службе кластеров предусмотрены два механизма обнаружения отказов, сигналы активности обнаружения отказов узлов и монитор с библиотекой ресурсов для обнаружения их отказов. Для обнаружения отказов узлов каждый узел периодически обменивается датаграммами с другими узлами кластера по частной сети кластера. Эти сообщения называются сигналами активности. Для обнаружения отказов ресурсов используются специальные мониторы, работающие совместно с диспетчером восстановления. Эти мониторы следят за состоянием ресурсов, периодически опрашивая их с помощью библиотек ресурсов. Когда монитор обнаруживает отказ ресурса, он извещает об этом диспетчера восстановления.

Следует заметить, что отказоустойчивость на уровне сервера является необходимым, но недостаточным условием обеспечения отказоустойчивости. Важно обеспечить отказоустойчивость на уровне настольной системы пользователя.

Когда обнаружен сбой на оборудовании узла, служба SQL Server отключается. Служба Cluster передает управление на другой узел и снова запускает службу SQL Server. Восстановление ресурсов на кластере происходит примерно через 15 с, однако при запуске службы SQL Server выполняется особый последовательный процесс, называемый возвращением к исходному режиму. Продолжительность этого процесса зависит от того, как было запрограммировано приложение. Если приложение запрограммировано восстанавливаемыми порциями, пользователь будет подключен через интервал восстановления программной порции плюс 15 с [14].

Перемещение журналов – это технология обеспечения отказоустойчивости серверов, реализуемая службой SQL Server, которая состоит в резервном копировании базы данных и восстановлении ее на другом сервере. Такая технология обеспечивает полную независимость друг от друга первичного и вторичного серверов (исключает сбои общего поля памяти). Недостатком ее является отсутствие механизма взаимного обнаружения сбоя и инициализации переключения на вторичный сервер [14].

Репликация сервера – это поддержка целого избыточного сервера, которая обеспечивает полную отказоустойчивость, поскольку защищает от любых аварий вплоть до полного разрушения одного из серверов [8]. Эта технология сложна по структуре и чаще используется в виде репликации транзакций с одного первичного сервера на один или несколько вторичных серверов. Достоинством технологии репликации транзакций является тот факт, что механизм репликации не пропускает поврежденные данные с первичного сервера на вторичный.

5. Аппаратно-программные средства обеспечения надежности средств коммуникаций

Методы достижения высокой надежности (отказоустойчивости) средств коммуникаций рассмотрим на примере отказоустойчивых коммутаторов Catalyst 6000 [15].

В коммутаторах Catalyst 6000 реализовано дублирование на уровне отдельных блоков (раздельное резервирование). Конструкция поддерживает избыточные модули супервизора, блоки питания, резервное подключение и в модели Catalyst 6500 коммутирующие матрицы. Все

компоненты системы, включая блоки питания, вентиляторы, модули супервизора и коммутируемые матрицы, рассчитаны на горячую замену без перерыва работы коммутатора.

В конфигурации с двумя супервизорами в случае отказа основного супервизора функция Cisco Fast Switchover немедленно передает управление коммутатором резервному супервизору в течение нескольких секунд. Резервный супервизор, синхронизированный с основным, сохраняет все настройки и использует копию действующего программного образа загрузки системы.

Для обеспечения высокой отказоустойчивости сети коммутаторы семейства Catalyst 6000 поддерживают протокол HSRP, который позволяет дублировать функции маршрутизации и в случае катастрофического отказа основного коммутатора быстро переключиться на резервный (общее резервирование). Средняя наработка на отказ таких коммутаторов составляет порядка 300 000 ч.

6. Аппаратно-программные средства обеспечения надежности сетевых каналов связи между ТС

Большой вклад в обеспечение надежности сетевых каналов связи вносит принцип обмена информацией по протоколам, которые предусматривают обмен пакетами с избыточным кодированием данных, реализующих безошибочную передачу информации. В случае обнаружения ошибки в данных пакет отбрасывается и автоматически передается повторно. Использование квитирования также вносит весомый вклад в надежность каналов связи.

Наиболее радикальным средством обеспечения надежности сетевых каналов связи является резервирование каналов. Реализация отказоустойчивого канала связи требует установки двух сетевых адаптеров и интеллектуального программного агента, непрерывно следящего за состоянием обоих адаптеров. При отказе компонентов одного из каналов управление в течение нескольких секунд передается на резервный канал и выдается сообщение об отказе одного из каналов.

Заключение

Надежность функциональных подсистем ИВС (как и отказоустойчивость) оценивается коэффициентом готовности, требования к которому достигают значения 0,99999 и более. Достижение такого значения коэффициента готовности возможно лишь при использовании раздельного резервирования компонентов ТС ИВС или общего резервирования (чаще дублирования) ТС.

Специфической особенностью ТС ИВС является тот факт, что восстановление работоспособности аппаратной части ТС не является достаточным для продолжения правильного функционирования ТС, требуется еще восстановление потерянной в результате отказа ТС информации.

В работе получены формулы расчета надежности отдельного ТС с учетом полноты самоконтроля работоспособности ТС и полноты сохранения информации, предшествующей моменту отказа ТС, а также формулы расчета надежности группы зарезервированных ТС с учетом полноты контроля работоспособности ТС и полноты сохранения информации на момент отказа ТС. Приведены способы аппаратной и программной поддержки надежности ТС ИВС при раздельном резервировании компонентов ТС и общем резервировании ТС ИВС.

Установлено, что для обеспечения высоких показателей надежности функциональных подсистем ИВС требуется обеспечить отказоустойчивость ТС ИВС. Отказоустойчивость ТС ИВС обеспечивается своевременным и достоверным контролем работоспособности компонентов ТС и ТС в целом, сокращением времени восстановления отказавших компонентов ТС и потерянной информации из-за отказа компонентов ТС или ТС в целом. Достоверность контроля обеспечивается систематическим мониторингом состояния ТС. Сокращение времени восстановления реализуется путем обеспечения горячей замены отказавших компонентов системы и за счет наличия комплектов запасных элементов. Время восстановления потерянной информации можно существенно сократить путем программирования приложений с образованием контрольных точек через небольшие интервалы работы программы.

Учитывая приведенные в работе аппаратно-программные методы обеспечения отказоустойчивости ТС ИВС, можно в настоящее время подобрать ТС для создания ИВС с очень высокими показателями надежности – до единиц минут непланового простоя ТС (группы ТС) в течение года.

Список литературы

1. Единая система стандартизации автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения: ГОСТ 24.701-86. – Минск: Изд-во стандартов, 1986. – 11 с.

2. Рубер, П. Какая отказоустойчивость достаточна / П. Рубер // LAN. Журнал сетевых решений. – 1998. – № 12. – С. 45–53.

3. Анищенко, В.В. Показатели и математическая модель надежности кластерного суперкомпьютера / В.В. Анищенко, Л.И. Кульбак, В.К. Фисенко // Информатика. – 2004. – № 2. – С. 5–12.

4. Коробейников, В. Сервер ЛВС семейства NetServer компании Hewlett Packard / В.В. Коробейников // PC Magazine/ Russian Edition. – 1996. – № 3. – С. 21–23.

5. Сердюк, О. Критерии выбора отказоустойчивых серверных систем / О. Сердюк // Банковское дело в Москве. – 1999. – № 9 (57). – С. 62–63.

6. Барсуков, Н. Компания Liebert-Hiross о новых моделях источников бесперебойного питания / Н. Барсуков [Электронный ресурс]. – 2001. – Режим доступа: http://business.compulenta.ru/13214/. – Дата доступа: 05.09.2007.

7. Каталог фирмы Portwell [Электронный ресурс]. – 2001. – Режим доступа: http://www.microset.ru /cataloginside.php?id=44&sc=FULLLIST&cl=4&iddevel=172&rd=3. – Дата доступа: 22.08.2007.

8. Штребе, М. Windows 2000: проблемы и решения. Специальный справочник / М. Штребе. – СПб.: Питер, 2002. – 864 с.

9. Каталог фирмы Octagon Systems [Электронный ресурс]. – 2007. – Режим доступа: http://www.prosoft.ru/catalog/octagon/. – Дата доступа: 21.09.2007.

10. Толковый словарь-справочник по компонентам памяти // Computer Direct. – 1996. – № 8.

11. Егоров, А. RAID 0, RAID 1, RAID 5, RAID 10 или что такое уровни RAID? / А. Егоров [Электронный ресурс]. – 2006. – Режим доступа: http://timcompany.ru/article4.html. – Дата доступа: 21.09.2007.

12. Диниколо, Д. Отказоустойчивость, анализ и настройка безопасности и IPSec / Д. Диниколо [Электронный ресурс]. – 2006. – Режим доступа: http://it-security.by.ru/doc/Win2000/12.html. – Дата доступа: 21.09.2007.

13. Гарбар, П. Организация отказоустойчивого хранилища / П. Гарбар // Открытые системы. – 2002. – № 4. – С. 12–21.

14. Хотек, М. Методы достижения высокой отказоустойчивости / М. Хотек // Windows IT Pro [Электронный ресурс]. – 2003. – Режим доступа: http://www.rnivc.kis.ru/?id=420. – Дата доступа: 15.08.2007.

15. Коммутаторы Cisco Catalyst [Электронный ресурс]. – 2007. – Режим доступа: http://www.abn.ru/catalog/cisco/a2.shtml. – Дата доступа: 05.10.2007.

Поступила 27.07.07

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова,6
e-mail: anishch@newman.bas-net.by

U.V. Anishchanka, L.I. Kulbak, T.S. Martsinovich

HARDWARE-SOFTWARE TOOLS OF INFORMATION SYSTEM RELIABILITY SUPPORT

Approaches and methods of hardware-software support of information system tools reliability are presented. Formulas of calculation of tools reliability indices and groups of the reserved tools in view of completeness of their condition control during work and information saving prior to hardware fault are given.