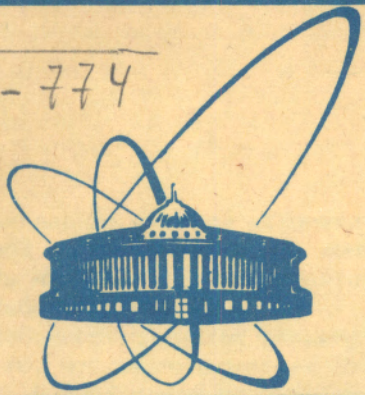

сообщения
объединенного
института
ядерных
исследований
дубна

Р10-81-309

А.И.Островной, И.М.Саламатин, Г.Я.Яновский

ОБРАБОТКА АВАРИЙНЫХ СИТУАЦИЙ В СИСТЕМЕ САНПО ДЛЯ ЭВМ ТИПА СМ-3

1981

Прикладные системы автоматического накопления и предварительной обработки данных в комплексе САНПО предназначены для работы на линии с экспериментальным оборудованием в реальном масштабе времени /1/.

Особенностью систем реального времени является, в частности, то, что возникающие в них ошибки носят случайный характер /2/. В этой связи особую важность приобретает проблема обеспечения надежности функционирования прикладных систем. Одним из основных аспектов этой проблемы является создание централизованных средств обработки аварийных ситуаций /3/.

Авторами была предпринята работа по обеспечению обработки аварийных ситуаций, которые могут возникнуть при исполнении программы эксперимента прикладной системой САНПО.

Аварийной ситуацией /АС/ мы называем такую ситуацию при работе системы, когда непосредственное продолжение исполнения может привести к непредсказуемым результатам /потеря управления, порча информации и т.п./. Ошибка определяется как идентификация факта аварийной ситуации.

Перед нами стояла задача создать единый унифицированный механизм обработки АС разной природы. Эти средства должны обеспечивать выдачу сообщений об ошибках при работе различных функциональных модулей прикладной системы /в том числе написанных на фортране-IV /, их интерпретацию с учетом организации работы прикладной системы, а также определенную реакцию на ошибку.

Работа выполнена для мини-ЭВМ с системой команд типа СМ-3 /4,5/.

1. ОБЩАЯ ОРГАНИЗАЦИЯ ОБРАБОТКИ АС

Для обработки АС при работе прикладной системы /ПС/ САНПО сформулирована и разработана подсистема. Такой подход соответствует общему направлению развития функциональных возможностей системы САНПО.

Подсистема обработки аварийных ситуаций /ПОАС/ предназначена для унифицированной обработки ошибок. Описываемая версия ПОАС осуществляет интерпретацию ошибки, обеспечивает формирование диагностического сообщения об ошибке, выдачу этого сообщения на терминал пользователя, принятие решения о продолжении или приостановке исполнения программы эксперимента в зависимости от вида АС.

09

1.1. По способу идентификации АС разделяются на две группы. К первой относятся такие ситуации при работе программного модуля, которые для реализуемого им алгоритма являются ошибочными, некорректными. Во время записи алгоритма программист предусматривает реакцию /например, вывод диагностического сообщения/ при обнаружении такой ситуации. В этом случае он формирует обращение к ПОАС в соответствии с определенными правилами, иными словами, объявляет ошибку.

Ко второй группе относятся АС, идентифицируемые процессором ЭВМ. Такие АС вызываются неверным обращением к оперативной памяти или попыткой использовать запрещенный код операции. Эти АС будем условно называть ошибками процессора. В таких случаях на ЭВМ типа СМ-3 возникает внутреннее аппаратное прерывание. Процессор ЭВМ прерывает текущую работу и передает управление программе, адрес входа в которую указан вектором прерывания с адресом оперативной памяти 4 или 10.

Данная подсистема обеспечивает обработку АС как первой, так и второй группы.

1.2. АС, по способу реакции на них, подразделяются на два типа: фатальные и нефатальные.

Мы определяем АС как фатальную, если исполнение программы, в которой АС обнаружена, не может быть продолжено. Напротив, для нефатальных АС, по определению, возможно продолжить исполнение программы после соответствующей обработки обнаруженной в ней АС.

Для фатальных АС итогом работы подсистемы является приостановка исполнения программы эксперимента, а для нефатальных - возврат управления в прерванную программу.

1.3. Для программирования обращения к ПОАС разработаны таблица классификации ошибок и последовательность обращения к подсистеме.

Таблица классификации предназначена для кодирования ошибок, объявляемых различными функциональными элементами ПС: монитором САНПО, подсистемами САНПО и стандартными программами /СП/.

Последовательность обращения к ПОАС определяет способ управления работой ПОАС со стороны функциональных модулей.

Обращение к ПОАС в случае АС производится с помощью команды TRAP. Команда TRAP имеет изменяемую часть, которую мы будем называть в дальнейшем номером. Номера этой команды могут принимать значения в диапазоне $0 \div 255_{10}$ [7]. Они должны использоваться в соответствии с разработанной таблицей классификации ошибок.

Обращение к подсистеме может содержать дополнительную информацию, характеризующую ошибку. Эта информация позволяет идентифицировать ошибку с точностью до функционального модуля

ПС: резидента монитора САНПО, резидентов подсистем или СП, получить информацию для вычисления адреса последней исполненной команды в этом модуле, а также определяет реакцию на ошибку.

Способ идентификации АС, которые могут возникнуть при работе СП, написанных на фортране, остается без изменений и осуществляется модулями стандартной фортранной библиотеки FORLIB [6] операционной системы RT-11 [7]. При обработке фортранных ошибок практически сохранен способ интерпретации и вид диагностических сообщений, принятые в системе RT-11 и описанные в справочных материалах по фортрану для системы RT-11 [6].

1.4. ПОАС имеет слово состояния, посредством которого, наряду с кодами дополнительной информации обращения, осуществляется управление работой подсистемы. Изменение слова состояния выполняется, как правило, в интерактивном режиме по приказам оператора. Назначение отдельных разрядов слова следующее:

Номер разряда	Функция		Значение
3	Печать сообщения об ошибке	Разрешена	1
		Запрещена	0
5	Печать текста описания ошибки	Разрешена	0
		Запрещена	1

Остальные разряды слова состояния являются резервными для данной версии подсистемы и содержат нулевой код.

Начальное значение слова состояния подсистемы - 10_8.

2. ОБЩАЯ СТРУКТУРА ПОДСИСТЕМЫ

2.1. В состав ПОАС входят специальный резидентный модуль монитора САНПО, резидент подсистемы и набор служебных СП.

Резидентный модуль монитора предназначен для минимальной обработки АС. Он всегда присутствует в оперативной памяти при работе ПС. Резидент подсистемы является основным средством обработки АС. Он обеспечивает интерпретацию ошибки, формирование сообщения об ошибке, выдачу его на терминал, а также обслуживает алгоритм принятия решения.

Служебные СП выполняют изменение функций подсистемы посредством модификации слова состояния и опрос его текущего состояния. Состав служебных СП подсистемы, форматы приказов, а также выполняемые ими функции описаны в Приложении 1.

2.2. ПОАС может работать в двух режимах: по минимальному и полному набору обслуживания. Если при работе ПС резидент подсистемы отключен, т.е. не был выполнен приказ SET("ERRRES"),

где ERRRES - имя резидента, то ПОАС работает по минимальному протоколу, обеспечивая вывод краткого сообщения об ошибке. Обработка ошибок процессора осуществляется монитором системы RT-11 или резидентным модулем монитора САНПО - для дисковой и перфоленточной версий ПС, соответственно.

В случае, когда резидент инициализирован, т.е. выполнен приказ SET("ERRRES")ПОАС обеспечивает обработку АС как первой, так и второй группы в полном объеме, определяемом функциональными возможностями подсистемы.

3. КЛАССИФИКАЦИЯ ОШИБОК

Таблица классификации ошибок разработана с целью упорядочить использование номеров команды TRAP при объявлении ошибок. А именно: данная классификация обеспечивает однозначное соответствие номера команды TRAP некоторому функциональному элементу /или группе элементов/ ПС.

Принято следующее распределение номеров команды TRAP.

Номер команды TRAP	Функциональная принадлежность
0÷6	Служебные коды прикладной системы
7	Резерв ПОАС
8_{10}÷15_{10}	Монитор САНПО
16_{10}	Подсистема управления с клавиатуры телетайпа
17_{10}	Подсистема обработки аварийных ситуаций
18_{10}	Подсистема для работы с оборудованием в стандарте КАМАК
19_{10}	Подсистема для работы с точечным дисплеем
20_{10}	Подсистема для работы с магнитной лентой
21_{10}÷127_{10}	Резерв системы САНПО
128_{10}÷159_{10}	Стандартные программы пользователей
160_{10}	Процессор ЭВМ
161_{10}÷191_{10}	Резерв
192_{10}÷255_{10}	Фортранные СП

Номера 0÷6 являются служебными. Они предназначены для организации исполнения программы эксперимента в ПС. Номер 7 зарезервирован для последующего развития описываемой подсистемы. Номер 160_{10} команды TRAP предназначен для объявления ошибок, приводящих к внутренним аппаратным прерываниям. Отметим, что по своему типу эти ошибки отнесены к фатальным.

Распределение остальных номеров команды TRAP подчинено следующему правилу: номер команды TRAP является признаком принадлежности модуля, в котором объявляется ошибка, к определенному функциональному элементу системы САНПО.

Номера 192_{10}÷255_{10} команды TRAP использованы для объявления ошибок из СП, написанных на фортране. Это правило вытекает из организации фортранной библиотеки FORLIB.

Программистам не рекомендуется использовать номера 0÷7, 160_{10}, 192_{10}÷255_{10} команды TRAP при написании СП.

4. ПОСЛЕДОВАТЕЛЬНОСТЬ ОБРАЩЕНИЯ К ПОДСИСТЕМЕ

Последовательность обращения к ПОАС предназначена для формирования обращения к подсистеме в случае обнаружения АС. Она предоставляет средства описания характеристик ошибок. Обращение состоит из последовательности кодов, заданных командами и директивами ассемблера MACRO-11.

Общая структура последовательности обращения к подсистеме показана на рис.1. Для программирования обращения к ПОАС введены следующие правила:

1. Слова 1 и 2 являются обязательными компонентами последовательности обращения;
2. Слова 3,4,5 последовательности обращения могут быть выборочно опущены;
3. Слова 3,4,5 присутствуют в последовательности обращения в определенном порядке: адрес возврата, адрес текста описания ошибки, адрес текста имени резидента некоторой подсистемы САНПО;
4. Состояние отдельных разрядов слова 2 является определяющим для реализации правила 2.

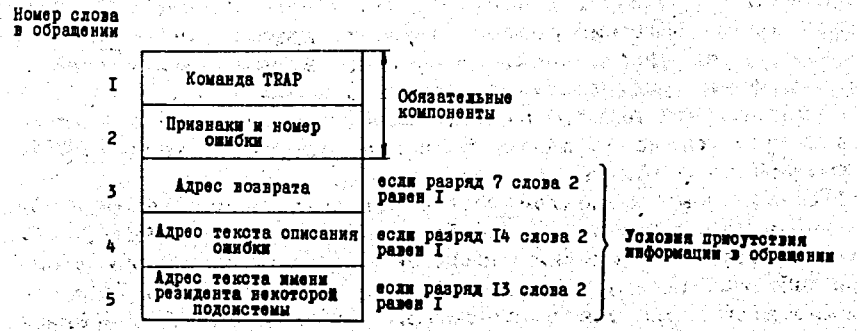

Рис.1. Структура последовательности обращения к подсистеме.

Первое слово последовательности обращения содержит код команды TRAP. Содержимое второго слова имеет структуру, при которой отдельные разряды или группы разрядов используются следующим образом:

Разряд	Назначение
0 ÷ 6	Код индивидуального номера ошибки
7	Тип ошибки
8 ÷ 11	Резерв
12	Признак ошибок, объявляемых резидентом монитора
13	Признак ошибок, объявляемых резидентами подсистем
14	Признак наличия текста описания ошибки
15	Резерв

Разряды 0 ÷ 6 этого слова содержат код, определяющий индивидуальный номер ошибки. Он может принимать значения от 1 до 127_{10}, нулевой код зарезервирован для развития описываемой подсистемы, и использовать его не рекомендуется. Номер команды TRAP и код индивидуального номера ошибки должны однозначно определять аварийную ситуацию.

Разряд 7 характеризует тип ошибки. Ошибка объявляется фатальной, если разряд 7 содержит нуль, а нефатальной - в противном случае.

Разряд 14 является признаком наличия текста описания ошибки. Его значение равно 1 в том случае, когда текстовое описание ошибки определенным образом сформировано и присутствует в программном модуле.

Резервные разряды слова 2 последовательности обращения должны содержать нулевые значения.

Разрядам 7, 14, 13 поставлены в соответствие адрес возврата, адрес текста описания ошибки и адрес текста имени резидента подсистемы САНПО в последовательности обращения к ПОАС. Согласно правилам 1÷4 программирования обращения к ПОАС, равенство этих разрядов единице означает присутствие в последовательности обращения соответствующих адресов /см. рис.1/. Если эти разряды равны нулю, то соответствующие данные должны быть опущены в последовательности обращения.

Отметим, что тексты описания ошибок, в также тексты имен резидентов подсистем должны быть представлены в коде ASCII и оканчиваться нулевым байтом.

Единственным элементом последовательности обращения к ПОАС при объявлении фортранных ошибок является команда TRAP. Тип каждой фортранной ошибки определен в таблице типов ошибки. Эта таблица, в силу ряда требований, изложенных в работе /8/, формируется в резиденте фортранной подсистемы САНПО. Таблица текстов описаний фортранных ошибок должна быть записана /под

именем ERRS с расширением MSG / в библиотеку ПС. При идентификации фортранной ошибки эта таблица может быть загружена в оперативную память для формирования сообщения об ошибке.

5. ОБРАБОТКА АВАРИЙНЫХ СИТУАЦИЙ В СИСТЕМЕ САНПО

5.1. Под обработкой АС в системе САНПО будем понимать действия, предпринимаемые ПОАС и имеющие целью способствовать функционированию ПС.

Функциональные возможности подсистемы характеризуют способы обработки АС. В данной версии ПОАС обработка АС включает:

1/ интерпретацию объявленной ошибки;

2/ определенный сервис для пользователя, заключенный в выдаче на терминал информации о характере ошибки и состоянии прерванной программы эксперимента;

3/ обеспечение, в благоприятных ситуациях, продолжения исполнения программы эксперимента.

5.2. Рассмотрим последовательность работы модулей ПОАС в процессе обработки АС.

При объявлении ошибки вектор прерывания команды TRAP обеспечивает передачу управления резидентному модулю монитора САНПО. Этот модуль в случае отключения резидента подсистемы всегда обеспечивает минимальную диагностику и передачу управления в соответствии с типом ошибки. Если резидент подсистемы инициализирован, модуль монитора передает ему управление.

Резидент выполняет анализ последовательности обращения, а также состояния ПС к моменту обнаружения ошибки. В результате резидент формирует и печатает диагностическое сообщение об ошибке и вырабатывает решение о продолжении или приостановке исполнения программы эксперимента.

Способ интерпретации ошибок, объявляемых из СП, написанных на фортране, учитывает организацию исполнения фортранных СП в системе САНПО. Известно /8/, что при передаче управления фортранной подпрограмме в стеке формируется элемент описания трассы передачи управления, характеризующий вызываемую подпрограмму. Элементы описания трассы используются для формирования сообщений о фортранных ошибках.

5.3. В данной версии ПОАС тип ошибки является определяющим параметром для принятия решения о продолжении или приостановке исполнения программы эксперимента.

В случае фатальных ошибок резидент подсистемы обеспечивает передачу управления подсистеме управления работой с клавиатуры телетайпа. Для нефатальных ошибок способ возврата управления в прерванную программу определяется функциональной принадлеж-

ностью номера команды TRAP в разработанной классификации. Для ошибок, объявляемых из фортранных СП, резидент обеспечивает передачу управления по адресу, следующему непосредственно за адресом команды TRAP. В остальных случаях /номер команды TRAP меньше 192_{10}/ резидент обеспечивает возврат управления по адресу, указанному в последовательности обращения к подсистеме. Если адрес возврата в последовательности обращения указан неверно, резидент печатает соответствующее сообщение и приостанавливает исполнение программы эксперимента.

6. ДИАГНОСТИЧЕСКИЕ СООБЩЕНИЯ И ИХ ФОРМАТЫ

Диагностические сообщения являются средством визуализации некоторой информации об ошибке, а также о состоянии ПС к моменту обнаружения ошибки.

Форматы сообщений определяются:

1/ составом ПОАС в прикладной системе;
2/ способом формирования обращения к подсистеме;
3/ составом последовательности обращения к ПОАС.

Схемы диагностических сообщений приведены на рис.2.

```
а) ?ERR N1,N2 < тип и адрес ошибки > [< текст описания ошибки >]
     IN   ROUTINE "NAME  "

б) ?ERR N [< текст описания ошибки >]
     IN   ROUTINE "SUBR3 "  LINE < номер строки >
     FROM ROUTINE "SUBR2 "  LINE < номер строки >
     FROM ROUTINE "NAME  "

в) ?ERR N [< текст описания ошибки >]
     IN   ROUTINE "SUBR3 "  LINE < номер строки >
     FROM ROUTINE "NAME  "

г) ?ERR N1,N2 < тип и адрес ошибки > [< текст описания ошибки >]
     IN   SANPO MON /?"NAME  "?/

д) ?ERR 160,N2 F/< адрес >/ [< текст описания ошибки >]
     /?"NAME  "?/

е) ?ERR N1,N2 < тип и адрес ошибки >

ж) ?ERR N
```

Рис.2. Схемы диагностических сообщений об ошибках.

6.1. Рассмотрим форматы сообщений, печатаемых резидентом ПОАС.

6.1.1. При объявлении ошибки из модуля, написанного на ассемблере, первая строка сообщений, в общем случае, содержит код и тип ошибки, адрес оперативной памяти, откуда выполнено обращение к подсистеме, и текст описания ошибки /рис.2а,г/. В этом случае код ошибки определяется двумя значениями: номером команды TRAP и индивидуальным номером ошибки. Два десятичных числа N_1 и N_2 в первой строке сообщения обозначают номер команды TRAP и индивидуальный номер ошибки, соответственно. Тип ошибки условно обозначается буквой F - для фатальных ошибок и буквой W - для нефатальных.

Вторая /последняя/ строка диагностического сообщения, в общем случае, содержит имя функционального модуля ПС, объявляющего ошибку /рис.2а,г/. Если ошибка объявляется резидентом монитора САНПО или резидентом некоторой подсистемы,эта строка сообщения содержит также имя СП /выделяемое косыми чертами/, подготовка или исполнение которой привели к АС /рис.2г/.

6.1.2. При объявлении ошибки из модуля, написанного на фортране, первая строка сообщения /рис.2б,в/ имеет структуру, совпадающую с описанной в справочных материалах по фортрану для системы RT-11 [6]. Код фортранной ошибки определяется одним параметром - номером команды TRAP. Десятичное число N в первой строке сообщения вычисляется по формуле:

$$N = N_{TR} - 192_{10},$$

где N_{TR} - десятичное представление номера команды TRAP.

Сообщения о фатальных и нефатальных ошибках имеют различный формат. В сообщении о фатальной ошибке /рис.2б/ содержится образ всей трассы передачи управления, сформированной к моменту объявления ошибки. В сообщении о нефатальной ошибке /рис.2в/ присутствует ссылка только на ту фортранную подпрограмму, при исполнении которой возникла соответствующая АС. Остальная часть описания трассы опускается.

Последние строки всех сообщений о фортранных ошибках содержат имена СП, при работе которых объявлены ошибки.

6.1.3. В отношении сообщений о так называемых ошибках процессора реализованы следующие положения:

а/ если сбой процессора произошел при работе модуля, написанного на ассемблере, то в последней строке сообщения/рис.2д/ указывается имя СП, подготовка к исполнению или работа которой привела к соответствующей АС;

б/ для ошибок процессора при исполнении СП, написанных на фортране, сохранена общая структура сообщений о фортранных ошибках /рис.2б/.

6.2. Резидентный модуль монитора САНПО всегда печатает минимальные сообщения об ошибках. Примеры таких сообщений приведены на рис.2е,ж. Эти сообщения совпадают с первыми строками соответствующих диагностических сообщений /рис.2а,б/, за исключением текстовых сообщений, которые опускаются.

7. ЗАКЛЮЧЕНИЕ

Данная подсистема обработки аварийных ситуаций предназначена для использования в системе автоматического накопления и предварительной обработки экспериментальных данных - САНПО.

Она обеспечивает унифицированный способ обработки АС, которые могут возникнуть при работе ПС САНПО.

Состав подсистемы и объем выполняемых ею функций может варьироваться в зависимости от наличных ресурсов ПС.

Управление работой ПОАС осуществляется двумя способами:

1/ автоматически в зависимости от параметров ошибки;

2/ приказами оператора с клавиатуры телетайпа.

Набор интерактивных приказов открыт и может пополняться по мере развития подсистемы.

Реализованная версия ПОАС обеспечивает интерпретацию ошибок, печать диагностических сообщений об ошибках и, в благоприятных ситуациях, возврат управления в прерванную программу для продолжения исполнения программы эксперимента.

Обеспечена обработка АС, возникающих в программах, работающих с экспериментальным оборудованием, в автоматически исполняемых процессах, а также в приказах оператора, инициированных в интерактивном режиме.

Для программирования обращения к ПОАС разработаны таблица классификации ошибок и последовательность обращения к подсистеме. Эти средства предоставляют удобный способ интерпретации ошибок, позволяют легко определять адрес оперативной памяти и модуль ПС, откуда выполнено обращение к подсистеме.

Реализованный алгоритм обработки АС, возникающих при исполнении СП, написанных на фортране, практически сохраняет способ идентификации и вид диагностических сообщений, которые описаны в справочных материалах по фортрану для операционной системы RT-11.

Развитие способов обработки АС в рамках ПОАС предполагает:

1/ разработку средств формирования архива статистики ошибок для последующего анализа работоспособности оборудования и программ;

2/ выработку рекомендаций, конкретизирующих область поиска причины АС;

3/ визуализацию состояния служебных областей и элементов данных ПС;

4/ организацию "спасения" максимально достоверной информации, накопленной в ходе эксперимента;

5/ запрограммированное изменение функций ПС во время исполнения программы эксперимента, что включает автоматическую перестройку алгоритма работы ПС вследствие, например, выхода из строя части второстепенного оборудования, регулярных сбоев при исполнении некоторой операции системы.

ПРИЛОЖЕНИЕ

Служебные СП подсистемы

Имя программы	Формат обращения	Выполняемая функция
ERMSG	ERMSG('ENABLE')	Разрешение формирования и печати сообщения об ошибке
	ERMSG('DISABLE')	Запрещение формирования и печати сообщения об ошибке
ERTXT	ERTXT('ENABLE')	Разрешение печати текста описания ошибки
	ERTXT('DISABLE')	Запрещение печати текста описания ошибки
ERSW	ERSW	Установка слова состояния подсистемы в исходное состояние (код ØØØØ1Ø)
	ERSW (восьмеричное число)	Занесение кода аргумента в слово состояния подсистемы
ERQMSG	ERQMSG	Опрос состояния указателя печати сообщения об ошибке
ERQTXT	ERQTXT	Опрос состояния указателя печати текста описания ошибки
ERQSV	ERQSV	Выдача на терминал текущего состояния слова состояния подсистемы (в восьмеричном виде)
ERQST	ERQST	То же (в текстовом виде)

ЛИТЕРАТУРА

1. Балука Г. и др. ОИЯИ, Р10-12960, Дубна, 1980.
2. Fergus P.J., Taylor J.M. High Integrity Systems. UKAEA, Report HL71/5799, 1971.
3. Ringland G. The Comp.Journ., 1975, vol.18, No.4, pp.312-317.
4. Наумов Б.Н., Боярченков М.А., Кабалевский А.Н. Приборы и системы управления, 1977, №10, с.12-15.
5. Наумов Б.Н. Приборы и системы управления, 1977, №10, с.3-5.
6. The RT-11 Fortran Compiler and Object Time System. User's Guide (DEC-11-LRFPA-A-D). DEC, Maynard, Massachusetts, 1975.
7. The RT-11 System Reference Manual (DEC-11-ORUGA-C-D). DEC, Maynard, Massachusetts, 1975.
8. Саламатин И.М., Яновский Г.Я. ОИЯИ, Р10-12971, Дубна, 1979.

Рукопись поступила в издательский отдел
7 мая 1981 года.