УДК 004.415:681.3

В.С. ХАРЧЕНКО, В.В. СКЛЯР, А.Х. АЛЬ-ТАРАЗИ

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

МОДЕЛИ СОСТОЯНИЙ И СОБЫТИЙ ОТКАЗОУСТОЙЧИВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ С УЧЕТОМ ИХ ВЛИЯНИЯ НА БЕЗОПАСНОСТЬ

Проанализирована эволюция свойств информационных и управляющих систем (ИУС), сделан вывод о развитии требований к их надежности: от требований к безотказности и готовности до требований к отказоустойчивости и отказобезопасности. Для оценки свойств отказоустойчивости и отказобезопасности разработаны модели состояний и событий ИУС, позволяющие дифференцировать состояния системы в соответствии с их влиянием на безопасность.

отказоустойчивость, безопасность, информационные и управляющие системы

Введение. Анализ проблемы отказобезопасности

Параллельно с эволюцией автоматических и автоматизированных ИУС, связанной прежде всего с наращиванием технических характеристик и возможностей их ядра – компьютерных средств, изменялись и свойства, которые отражали способность ИУС выполнять заданные функции. В 50-е годы речь шла о безотказности этих средств, которая являлась основной составляющей надежности. Далее, в 60–70-е годы, когда стало ясно, что отказы ИУС неизбежны, а следовательно, необходимо обеспечивать способность систем функционировать в условиях их накопления, появились понятия "отказоустойчивость" и "отказоустойчивые системы" [1, 2]. Свойство отказоустойчивости представляло собой некую альтернативу свойству готовности для ИУС реального времени, восстановление работоспособности должно проходить автоматически в неограниченном временном интервале. По мере увеличения влияния программных средств на надежность ИУС и вследствие других причин в англоязычной литературе в 80-е годы был введен термин "dependability", который получил русскоязычный аналог – "гарантоспособность" [3 – 5]. Фактически он соответствовал свойству надежности в широком смысле, включающему не только ее канонические составляющие (безотказность, ремонтопригодность, долговечность, сохраняемость), но и отказоустойчивость, обслуживаемость, живучесть, безопасность (как в смысле "safety", так и в смысле "security") [6 – 8]. Следует подчеркнуть, что нарастание технической составляющей в спектре причин аварий и катастроф и увеличение весомости ИУС как объекта и средства поддержания безопасности привело к тому, что стало естественным использование еще одного термина и соответствующего свойства – отказобезопасности. Оно объединяет две составляющие гарантоспособности – отказоустойчивость и безопасность (в смысле "safety") и является, на наш взгляд, исключительно важным для ИУС комплексов критического применения. Элементы теории отказобезопасных систем, их автоматные модели, методы обеспечения отказобезопасности для различных приложений нашли отражение в литературе [9 – 11].

Кроме того, в работах [12 – 15] были предложены модели ИУС, учитывающие отказы программных и аппаратных компонент, а также решающих устройств.

Однако применительно к ИУС остается нерешенным вопрос формирования их модельной базы, в том числе с учетом всего набора состояний и переходов между ними (событий) для объекта контро-

ля и управления, а также для устройств, осуществляющих управление и контроль.

Цель данной статьи – разработка моделей состояний и событий отказоустойчивых ИУС, позволяющих дифференцировать состояния системы в соответствии с их влиянием на безопасность.

Общая модель ИУС

Далее рассматриваются ИУС, устройства и объекты контроля и управления (ОКУ).

Будем считать, что ИУС содержит устройство контроля (УК), идентифицирующие средства состояния ОКУ и устройство управления (УУ), переводящее объект при необходимости в безопасное состояние (рис. 1). Между УК, УУ и ОКУ осуществляется обмен информацией.

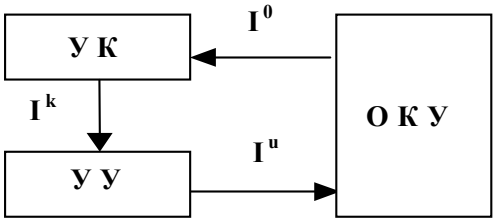

Рис. 1. Общая модель ИУС

Общую модель ИУС целесообразно дополнить компонентной моделью (рис. 2). Ядром ИУС являются программно-технические комплексы (ПТК), включающие в себя технические средства (ТС) и программное обеспечение (ПО). Кроме ПТК ИУС также включает в себя датчики (входят в состав УК) и исполнительные механизмы (входят в состав УУ).

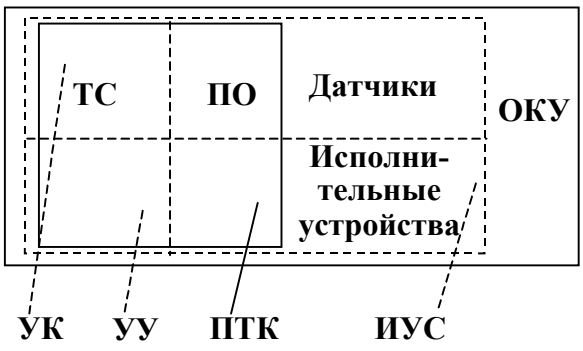

Рис. 2. Компонентная модель ИУС

Модель состояний ИУС

Множество состояний MS, в которых может находиться любая система, определяется в соответствии с [12, 13] выражением

$$MS = \{S_И, MS_{НИР} = \bigcup_{i=1}^{n_{НИР}} S_{НИРi}, MS_{ЧР} = \bigcup_{j=1}^{n_{ЧР}} S_{ЧРj},$$

$$MS_{НРБ} = \bigcup_{k=1}^{n_{НРБ}} S_{НРБk}, MS_{НРО} = \bigcup_{m=1}^{n_{НРО}} S_{НРОm} \},$$

где $S_И$ – исправное состояние; $MS_{НИР}$, $MS_{ЧР}$, $MS_{НРБ}$, $MS_{НРО}$ – множества неисправных работоспособных, частично работоспособных, неработоспособных безопасных и опасных состояний, соответственно, для любых пар различных элементов, для которых справедливо $S_{\nu\mu} \cap S_{\eta\omega} = 0$; $MS_Р = S_И \cup M_{НИР}$, $MS_{НР} = MS_{НРБ} \cup MS_{НРО}$ – множества работоспособных (полностью работоспособных) и неработоспособных (частично неработоспособных) состояний соответственно; $n_{НИР}$, $n_{ЧР}$, $n_{НР}$ – мощности соответствующих множеств.

Информация об истинном состоянии (ИС, S_i) ОКУ $\mathbf{I^0}$ поступает в УК, которое формирует данные о распознанном состоянии (РС, $\overline{S_j^0}$) объекта $\mathbf{I^k}$, по которым УУ выдает управляющие сигналы $\mathbf{I^u}$ (см. рис. 1), определяющие его переход в устанавливаемое состояние (УС, $\overline{\overline{S_p^0}}$). Состояния S_i^0, $\bar{S}_j^0$, $\bar{\bar{S}}_p^0$ принадлежат множествам MS^0, $M\bar{S}^0$, $M\bar{\bar{S}}^0$ соответственно, которые идентичны по составу элементов и имеют равную мощность.

Каждое из этих множеств имеет также тупиковое состояние $S_0(S_0^0, \bar{S}_0^0, \bar{\bar{S}}_0^0)$, соответствующее ситуации, когда информация на выходах ОКУ, УК и УУ либо отсутствует, либо является неидентифицируемой с точки зрения возможных состояний этих средств, т.е.

$$MS^0 = S_0^0 \cup MS_{ДП}^0, \quad M\bar{S}^0 = \bar{S}_0^0 \cup M\bar{S}_{ДП}^0,$$

$$M\bar{\bar{S}}^0 = \bar{\bar{S}}_0^0 \cup M\bar{\bar{S}}_{ДП}^0,$$

где $MS^0_{ДП}$, $M\bar{S}^0_{ДП}$, $M\bar{\bar{S}}^0_{ДП}$ – множества допустимых состояний ОКУ, УК, УУ (т.е. состояний, введенных при построении модели, исходя из множества допустимых отказов этих средств).

В общем случае

$$\text{Card } MS^0 \geq \text{Card } M\bar{S}^0 \geq \text{Card } M\bar{\bar{S}}^0.$$

Это объясняется тем, что идентификация истинных состояний ОКУ может проходить с меньшей разрешающей способностью, достаточной для решения задачи контроля в данной системе, а подмножеству распознаваемых состояний может соответствовать одно устанавливаемое состояние.

Состояния из множеств MS^0 , $M\bar{S}^0$, $M\bar{\bar{S}}^0$ изменяются во времени. Истинное состояние $S^0_i(t)$ в момент времени t распознается в момент времени $t+\tau_k$, т.е. распознанное состояние, формируемое УК, – это состояние $\bar{S}^0_j(t+\tau_k)$. Устанавливаемое состояние формируется УУ в момент времени $(t+\tau_k+\tau_u)$ – $\bar{\bar{S}}^0_p(t+\tau_k+\tau_u)$. В течение времени $+\tau_o$ происходит изменение состояния ОКУ. Цикл контроля и управления есть сумма времени:

$$T_{ку} = \tau_k+\tau_u+\tau_o = +\tau_{ko}+\tau_o.$$

При этом $\tau_{ko} = \tau_k+\tau_o$ должно быть не больше допустимого времени $\tau_{kuДОП}$.

Для объекта контроля и управления может быть выделено также множество потенциально опасных состояний $MS^0_{ПО} = \bigcup_{q=1}^{n_{ПО}} S^0_q$, из которых наиболее вероятен переход в одно из состояний $S^0_p \in M^0_{НРО}$. Вероятность перехода может определяться качественным путем. Например, к потенциально опасным могут быть отнесены состояния, для которых существуют элементы, отказ которых ведет к переходу в опасное состояние. Элементы множества $MS^0_{ПО}$ входят в подмножества множеств $MS^0_{НИР}$, $MS^0_{ЧР}$, $MS^0_{НРБ}$:

$$MS^0_{ПО} = MS^0_{НИР/ПО} \cup MS^0_{ЧР/ПО} \cup MS^0_{НРБ/ПО},$$

где $MS^0_{НИР/ПО} = MS^0_{НИР} \cap MS^0_{ПО}$,

$MS^0_{ЧР/ПО} = MS^0_{ЧР} \cap MS^0_{ПО}$,

$MS^0_{НРБ/ПО} = MS^0_{НРБ} \cap MS^0_{ПО}$.

Графическая модель состояний ИУС представлена на рис. 3.

Таким образом, состоянием ИУС будем называть кортеж

$$S^S_i(t) = <S^0_i(t),\ S^k_j(t+\tau_k),\ S^u_p(t+\tau_{k+}\tau_u)>,$$

где $S^0_i(t) \in MS^0,\ S^k_j(t+\tau_k) \in MS^k,$

$$S^u_p(t+\tau_{k+}\tau_u) \in MS^u.$$

Обычно

$$\frac{\text{Card}M^0_{НРБ/ПО}}{\text{Card}M^0_{НРБ}} \geq \frac{\text{Card}^0_{ЧР/ПО}}{\text{Card}^0_{ЧР}} \geq \frac{\text{Card}^0_{НИР/ПО}}{\text{Card}^0_{НИР}}.$$

Устройства контроля и управления как и объекты контроля и управления могут находиться в разных технических состояниях (исправном, неисправном, работоспособном, частично работоспособном, неработоспособном, безопасном и опасном), образующих множества MS^k и MS^u соответственно. Состояния $S^k_j \in MS^k$ и $S^u_p \in MS^u$ так же, как и состояния $\bar{S}^0_p$ и $\bar{\bar{S}}^0_q$, могут быть привязаны ко времени $t+\tau_k$ и $t+\tau_{k+}\tau_u$ соответственно.

Следует подчеркнуть, что пары состояний $\bar{S}^0_p$ и S^k_j ($\bar{\bar{S}}^0_q$ и S^u_p) взаимосвязаны, поскольку в случае отказа УК (УУ) нарушается соответствие между состояниями $S^0_i \in MS^0$ и $\bar{S}^0_k \in M\bar{S}^0$ ($\bar{S}^0_k \in M\bar{S}^0$ и $\bar{\bar{S}}^0_k \in M\bar{\bar{S}}^0$).

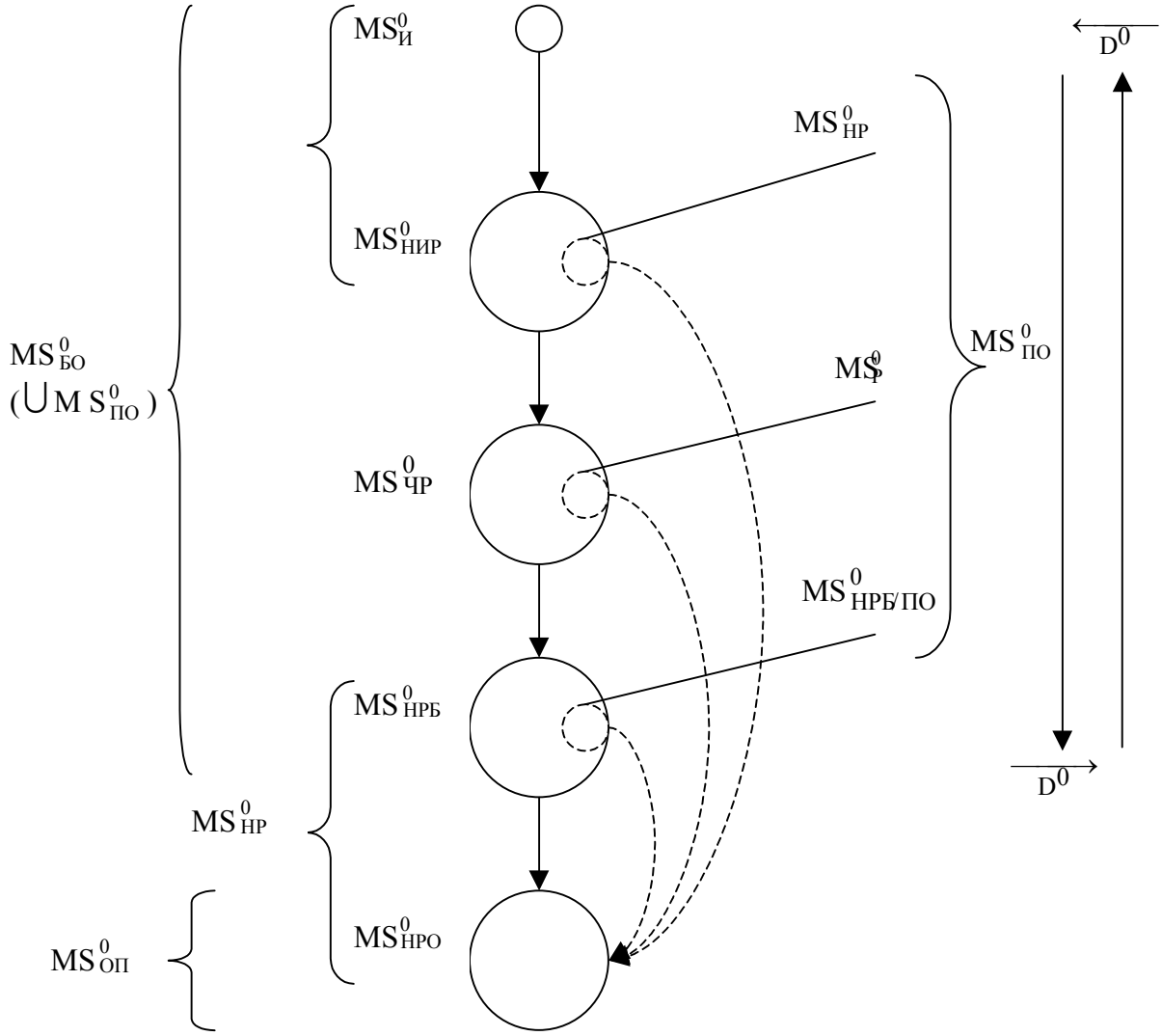

Рис. 3. Модель состояний ИУС

Множество состояний ИУС MS^s в момент времени t представляет собой декартово произведение множеств состояний объекта, средств контроля и средств управления:

$$MS^s(t)=MS^0(t) \times MS^k(t+\tau_k) \times MS^0(t+\tau_{ko}).$$

Множество состояний системы образует таким образом трехмерное пространство состояний (рис. 4).

Очевидно, что множества

$$MS^S_n(t)=\{<S^0_n(t), S^k_n(t+\tau_k), S^u_n(t+\tau_{ko})>\};$$

$$MS^S_{НИР}(t)=\{<S^0_{НИРi}(t), S^k_{НИРi}(t+\tau_k),$$

$$S^u_{НИРi}(t+\tau_{ko})>, i=\overline{1, n_{НИР}}\};$$

$$MS^S_{ЧР}(t)=\{<S^0_{ЧРj}(t), S^k_{ЧРj}(t+\tau_k), S^u_{ЧРj}(t+\tau_{ko})>,$$

$$i=\overline{1, n_{ЧР}}\}$$

определяют исправное, неисправное работоспособные и частично работоспособное состояния ИУС. Совпадение индексов для элементов кортежей множеств $MS^S_{НИР}(t)$ и $MS^S_{ЧР}(t)$ указывает на безошибочное функционирование УК и УУ.

В общем случае множество неисправных работоспособных состояний ИУС описывается выражением

$$MS^S_{НИР}=MS^S_p \setminus MS^S_и,$$

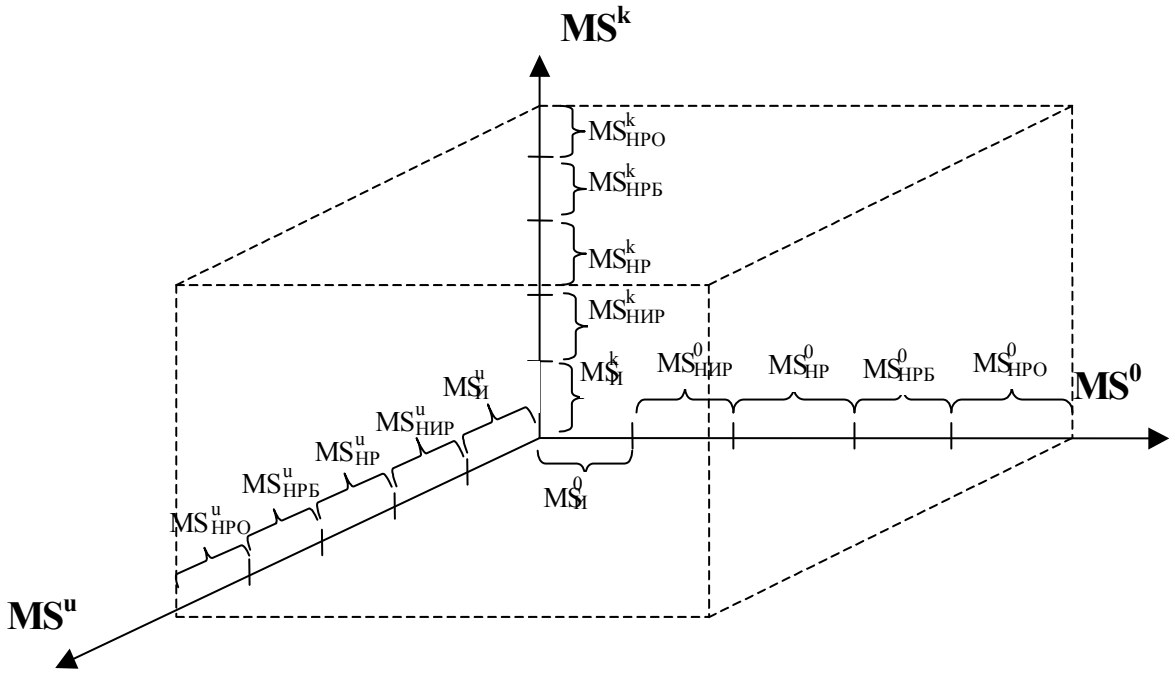

Рис. 4. Пространство состояний ИУС

где $MS^{S}_{p} = \{<S^{0}_{j} \in MS^{0}_{p}, S^{k}_{j} \in MS^{k}_{p},$

$S^{u}_{j} \in MS^{u}_{p}>\}$, т.е. $MS^{S}_{НИР} \supset MS^{S}_{НИР}$.

Аналогично полное множество частично работоспособных состояний системы определяется следующим образом:

$$MS^{S}_{ЧР} = MS^{S}_{ЧР} \setminus MS^{S}_{p},$$

где $MS^{S}_{ЧР} = \{<S^{0}_{j} \in (MS^{0}_{p} \cup MS^{0}_{ЧР}),$

$S^{k}_{j} \in (MS^{k}_{p} \cup MS^{k}_{Ч}), S^{u}_{j} \in (MS^{u}_{p} \cup MS^{u}_{ЧР})>\}$.

Введенные понятия позволяют формализовать описание опасного состояния ИУС. ИУС находится в опасном состоянии, если в опасном состоянии находится объект контроля и управления, а УУ не формирует в течении допустимого времени переход ОКУ в безопасное состояние, либо УУ вследствие отказа формирует переход объекта в опасное состояние, т.е.

$S^{S}_{i}(t) \in MS^{S}_{НРО}: \{[S^{0}_{j}(t) \in MS^{0}_{НРО}]\&$

$\&[S^{u}_{r}(t+\tau_{ku}) \in MS^{u}_{НРБ}, \tau_{ku} > \tau_{kuДОП}]\} \vee$

$\vee \{[S^{0}_{j}(t) \in MS^{0}_{НРО}]\&$

$\&[S^{u}_{r}(t+\tau_{ku}) \notin MS^{u}_{НРБ}]\} \vee \{S^{u}_{r} \in MS^{u}_{НРО}\}$.

Другими словами, опасному состоянию ИУС $S^{0}_{НРО}$ соответствуют кортежи:

$< S^{0}_{НРОi}, \sim, S^{u}_{j} \notin MS^{u}_{НРБ} >$;

$< S^{0}_{НРОi}(t), \sim, S^{u}_{НРБj}(t+\tau_{ku}) >$;

$<\sim, \sim, S^{u}_{НРОj}>$.

В табл. 1 приведены все возможные варианты комбинаций состояний ОКУ, УК и УУ и соответствующие им состояния ИУС при условии, что УК и УУ не могут находиться в частично работоспособном состоянии.

Таблица 1

Возможные состояния ИУС и ее компонент

Состояние			Состояние ИУС
ОКУ	УК	УУ	
$S^0_{И}$	$S^k_{И}$	$S^u_{И}$	$S^S_{И}$
$S^0_{И}$	$S^k_{НИР}$	$S^u_{И}$	$S^S_{НИР}$
$S^0_{И}$	$S^k_{И}$	$S^u_{НИР}$	$S^S_{НИР}$
$S^0_{И}$	$S^k_{НИР}$	$S^u_{НИР}$	$S^S_{НИР}$
$S^0_{НИР}$	$S^k_{И}$	$S^u_{И}$	$S^S_{НИР}$
$S^0_{НИР}$	$S^k_{И}$	$S^u_{НИР}$	$S^S_{НИР}$
$S^0_{НИР}$	$S^k_{НИР}$	$S^u_{И}$	$S^S_{НИР}$
$S^0_{НИР}$	$S^k_{НИР}$	$S^u_{НИР}$	$S^S_{НИР}$
$S^0_{ЧР}$	$S^k_{И}$	$S^u_{И}$	$S^S_{ЧР}$
$S^0_{ЧР}$	$S^k_{И}$	$S^u_{НИР}$	$S^S_{ЧР}$
$S^0_{ЧР}$	$S^k_{НИР}$	$S^u_{И}$	$S^S_{ЧР}$
$S^0_{ЧР}$	$S^k_{НИР}$	$S^u_{НИР}$	$S^S_{ЧР}$
$S^0_{НРО}$	~	~	$S^S_{НРО}$

Модель событий ИУС

В процессе функционирования в объекте могут возникнуть отказы (сбои), которые приводят к его переходам в пространстве состояний MS^0. При восстановлении отказавших элементов или устранении сбоев объект переходит в состояние с более высоким уровнем работоспособности. Будем называть переходы первого типа движением ОКУ вниз ($\xrightarrow[D^0]{}$), а переходы второго типа – движением ОКУ вверх ($\xleftarrow[D^0]{}$) (см. рис. 3).

Движения ОКУ $\xrightarrow[D^0]{}$ и $\xleftarrow[D^0]{}$ представляют собой множество переходов:

$$\xrightarrow[D^0]{} = \{ S^0_{Hi} \to S^0_{НИРj} \vee S^0_{ЧРk} \vee S^0_{НРm} ,$$

$$S^0_{НИРj} \to S^0_{ЧРk} \to S^0_{ЧРk} \vee S^0_{НРm} , S^0_{ЧРk} \to$$

$$\to S^0_{НРm} , S^0_{НРБр} \to S^0_{НРОq} \};$$

$$\xleftarrow[D^0]{} = \{S^0_{НРОq} \to S^0_{НРБр} \vee S^0_{ЧРk} \vee$$

$$\vee S^0_{НИРj} \vee S^0_{Иi} , S^0_{НРБр} \to S^0_{ЧРk} \vee S^0_{НИРj} \vee S^0_{Иi} ,$$

$$S^0_{ЧРk} \to S^0_{НИРj} \vee S^0_{Иi} , S^0_{НИРj} \to S^0_{Иi} \}.$$

Движение $\xrightarrow[D^0]{}$ состоит из безопасных, потенциально опасных и опасных движений:

$$\xleftarrow[D^0]{} = \xrightarrow[D^O_{БО}]{} \cup \xrightarrow[D^O_{ПО}]{} \cup \xrightarrow[D^O_{ОП}]{},$$

где $\xrightarrow[D^O_{БО}]{}$ – переходы в состояния

$S^0_i \in (MS^0_{ЧР} \cup MS^0_{НРБ}) \setminus MS^0_{ПО}$;

$\xrightarrow[D^O_{ПО}]{}$ – переходы в состояния $S^0_j \in MS^0_{ПО}$;

$\xrightarrow[D^O_{ОП}]{}$ – переходы в состояния $S^0_k \in MS^0_{НРО}$.

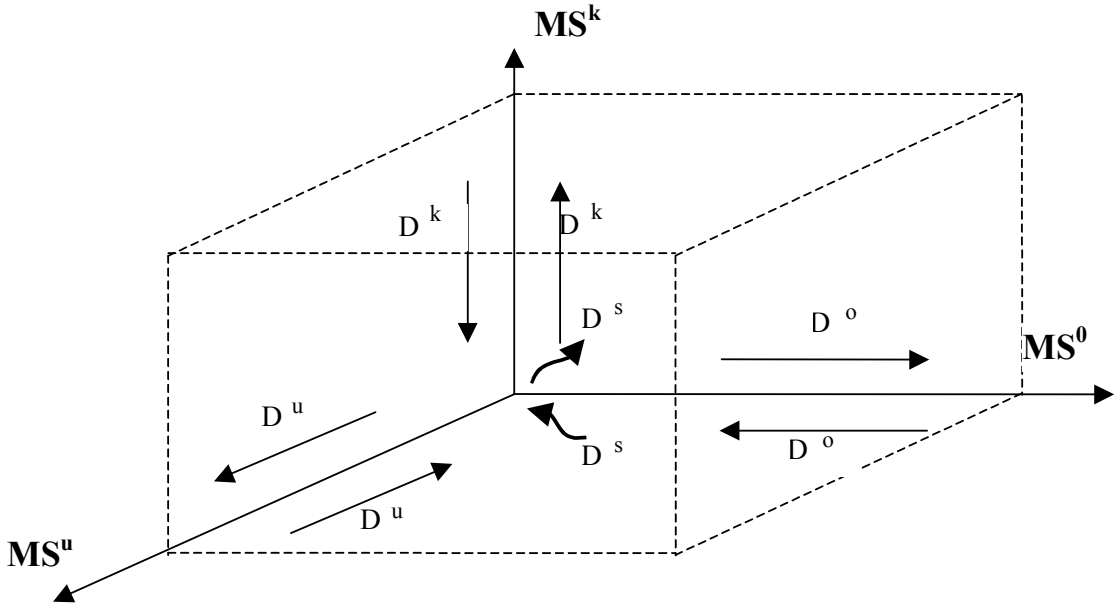

Рис. 5. Модель событий переходов (движения) ИУС в пространстве состояний

Аналогично могут быть определены движения вверх из опасных, потенциально опасных и безопасных состояний.

Однако такое ухудшение качества имеет место только при переходах во множество частично работоспособных или неработоспособных состояний и описывается моделью многоступенчатой деградации. По аналогии процессы восстановления (редеградации) $\underset{D^{O}_{РД}}{\longleftarrow}$ являются подмножеством движения вниз, т.е.

$$\underset{D^{O}_{ДГ}}{\longrightarrow} \subset \underset{D^{O}}{\longrightarrow},$$

$$\underset{D^{O}_{РД}}{\longleftarrow} \subset \underset{D^{O}}{\longleftarrow}.$$

Движения вниз и вверх для УК и УУ определяются аналогично и представляют собой множества $\underset{D^{k}}{\longrightarrow}$, $\underset{D^{k}}{\longleftarrow}$, $\underset{D^{u}}{\longrightarrow}$, $\underset{D^{u}}{\longleftarrow}$ соответственно.

По аналогии с движением ОКУ, УК и УУ может быть введено понятие движения ИУС, которое определяется как суперпозиция движений объекта и устройств контроля и управления в пространстве возможных состояний (рис. 5). Траектория движения определяется исходным и конечным состояниями системы. Это состояние фиксируется в соответствии с табл. 1.

Заключение

Свойства ИУС и требования к ним, связанные с поддержкой заданного технического состояния, эволюционировали по схеме "от безотказности (готовности) к отказоустойчивости и отказобезопасности". Требования к безотказности предполагают максимально возможное отдаление момента отказа элементов и системы, а при его наступлении – восстановление путем ремонта или замены отказавших компонент. Свойство отказоустойчивости базируется на понимании неизбежности отказов и введении средств, делающих ИУС нечувствительной к отказам элементов в течение максимального времени. Для комплексов критического применения важнейшим является свойство отказобезопасности, которое обеспечивает возможность перехода системы в безопасное состояние при любых отказах элементов.

Предложенные модели отказоустойчивых ИУС включают в себя:

– модель состояний (см. рис. 3), отличающуюся учетом всего множества состояний как объекта, так и устройств (средств) контроля и управления (исправных, неисправных работоспособных, частично работоспособных, неработоспособных, безопасных и опасных);

– модель пространства состояний (см. рис. 4, табл. 1), связанных с различными типами отказов компонент системы;

– модель событий переходов (движения) ИУС в пространстве возможных состояний объекта и устройств контроля и управления (см. рис. 5).

Для уменьшения вероятности опасных ошибок и перехода объекта в опасное состояние, модели которого следует разработать в дальнейшем, кратность резервирования средств, глубина и оперативность контроля должны быть достаточными для автоматического блокирования такого перехода. Средства контроля и управления должны регулярно демонстрировать свою способность выполнять функции, поддерживающие отказоустойчивость.

Литература

1. Avizienis A. Fault-tolerance: the survival attribute of digital systems // IEEE Transactions of Computers. – 1978. – V. 66, № 10. – P. 1109–1026.

2. Доманицкий С.М. Построение надежных логических устройств. – М.: Энергия, 1971. – 280 с.

3. Авиженис А., Лапри Ж.-К. Гарантоспособные вычисления: от идей до реализации в проектах // ТИИЭР. – 1986. – Т. 74. – № 5. – С. 8 – 21.

4. Лонгботом Р. Надежность вычислительных систем. – М.: Энергоатомиздат, 1985. – 288 с.

5. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. – М.: Радио и связь, 1989. – 208 с.

6. Березюк Н.Т., Галунин А.Я., Подлесный Н.И. Живучесть микропроцессорных систем управления. – К.: Техника, 1988. – 143 с.

7. Leveson N. Safeware: System Safety and Computers. – Addison-Wesley, 1995. – 431 p.

8. Laprie J.-C. Dependability Handbook. LAAS Report n 98-346. – Toulouse: Laboratory for Dependability Engineering, 1998. – 365 p.

9. Дружинин Г.В. Надежность автоматизированных производственных систем. – М.: Энергоатомиздат, 1986. – 480 с.

10. Додонов А.Г. Введение в теорию живучести вычислительных систем. – К.: Наук. думка, 1990. – 184 с.

11. Многоверсионные системы, технологии, проекты / В.С. Харченко, В.Я. Жихарев, В.М. Илюшко, Н.В. Нечипорук. – Х.: НАКУ «ХАИ», 2003. – 486 с.

12. Харченко В.С., Зенин А.П., Скляр В.В. Методы многопараметрической адаптации бортовых управляющих и вычислительных систем с раздельным мажоритарным резервированием // Космічна наука і технологія. – 1999. – Т. 5, № 5-6. – С. 81 – 91.

13. Харченко В.С., Скляр В.В. Графово-событийная модель для оценки надежности и последовательность выбора архитектур адаптивных многоверсионных систем // Інформаційно-керуючі системи на залізничному транспорті. – 2000. – № 4. – С. 64–67.

14. Скляр В.В., Харченко В.С. Отказоустойчивые компьютерные системы управления с версионно-пороговой адаптацией: Способы адаптации, оценка надежности, выбор архитектур // Автоматика и телемеханика. – 2002. – № 6. – С. 131–145.

15. Харченко В.С., Скляр В.В., Токарев В.И. Модели отказобезопасных структур цифровых систем контроля и управления // Системи обробки інформації. – Х.: ХВУ. – 2003. – Вип. 4. – С. 200 - 205.

Поступила в редакцию 25.03.04

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский государственный технический университет сельского хозяйства, г. Харьков