УДК 004.052

А.А. Орехова, В.С. Харченко, Е.В. Брежнев, В.О. Бутенко

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

РАЗРАБОТКА МАРКОВСКИХ МОДЕЛЕЙ ГОТОВНОСТИ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ С УЧЕТОМ ХАРАКТЕРИСТИК ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА

Анализируется класс информационно-управляющих систем, в которых ошибки оператора или дефекты человеко-машинного интерфейса могут привести к переходу системы в состояния безопасного и опасного отказов. Предложены марковские модели готовности информационных и управляющих систем, учитывающие характеристики человеко-машинного интерфейса и ошибки оператора. Приводятся точечные результаты исследования марковских моделей готовности с помощью пакета программ Mathematica.

Ключевые слова: *информационно-управляющие системы, человеко-машинный интерфейс, марковские модели, готовность.*

Введение

Для исследования надежности и безопасности информационно-управляющих систем (ИУС) широкое распространение получили методы, основанные на использовании аппарата теории случайных марковских процессов [1 – 3]. Как правило, отказы ИУС связывают с отказами их аппаратно-программных компонент. В интерактивных информационно-управляющих системах человеко-машинный интерфейс (ЧМИ) представляет отдельную подсистему, через которую оператор контролирует состояние объекта и управляет им в определенных режимах. С помощью ЧМИ оператор может не только обнаруживать отказы в системе, но и устранять их. Однако ошибочные действия самого оператора могут, наоборот, переводить систему из работоспособного состояния в состояние отказа [4]. Отдельные результаты применения марковских моделей для исследования интерактивных систем с учетом ЧМИ приводятся в работах [5 – 7]. Однако, в этих работах детализация описания состояний с учетом различных последствий ошибочных действий оператора и дефектов ЧМИ не проводилась.

Целью данной работы является обоснование и разработка марковских моделей готовности ИУС с учетом человеко-машинного интерфейса.

Структурная модель интерактивной информационно-управляющей системы

Структурная модель типовой информационно-управляющей системы показана на рис. 1.

Аппаратно-программные компоненты распределенной ИУС включают в себя локальную вычислительную сеть, сервера, множество шлюзовых компьютеров, при помощи которых ИУС присоединяется к другим подсистемам. ЧМИ таких систем реализован на базе рабочих станций (РС), предназначенных для контроля и управления (например, реактора АЭС), а также администрирования и контроля программных и технических средств ИУС.

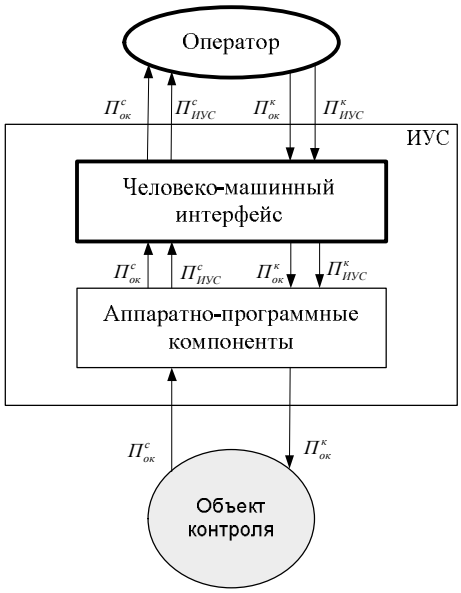

Рис. 1. Обобщенная структура типовой информационно-управляющей системы

ИУС осуществляет обработку четырех информационных потоков:

$П^{с}_{ок}$ - поток сигналов контроля состояния объекта;

$П^{к}_{ок}$ - потока команд управления оборудованием объекта;

$П^{с}_{ИУС}$ - поток сигналов диагностики состояния самой ИУС;

$П^{к}_{ИУС}$ - поток команд управления ИУС.

Поток сигналов контроля $П^{с}_{ок}$ формируется в системе низовой автоматики и после фильтрации,

сжатия и сохранения на сервере передается оператору через ЧМИ. В функции РС входит отображение поступающей информации в сжатой проблемно-ориентированной форме, которая зависит от решаемых операторами задач.

Поток команд управления $П^{к}_{ок}$ оборудованием начинается на рабочих станциях и передается в соответствующие подсистемы. Поток сигналов о состоянии ИУС $П^{с}_{ИУС}$ формируется во всех ее элементах и поступает на ЧМИ инженерных РС.

Поток сигналов управления ИУС $П^{к}_{ИУС}$ формируется в инженерных РС и содержит команды по управлению элементами ИУС.

Современные ИУС (например, АЭС) обладают следующими характеристиками [8] :

- количество аналоговых сигналов может доходить до нескольких тысяч; дискретных сигналов – до 100 тысяч, диагностических до 400 тысяч;
- средняя наработка на отказ подсистемы не менее 10^5 часов;
- коэффициент неготовности подсистемы не более 10^{-5} часов;
- время обновления информации на экранах дисплеев должно быть не более 1 секунды;
- время передачи команд управления – не более 2 секунд.

При анализе надежности интерактивных систем необходимо учитывать ошибки оператора. В процессе работы оператор с помощью ЧМИ воспринимает информацию, диагностирует состояние станции и технологического оборудования, принимает решение и выполняет определенные действия. На каждом из этих этапов возможны ошибки оператора. Источником опасных действий на этапе восприятия информации может быть поток сигналов, превышающий возможности человека, или восприятие искаженных данных. Большой объем несущественной информации на ЧМИ, определяющий высокую рабочую нагрузку, может быть причиной неверной идентификации состояния технологического контура. Отсутствие информации о наличии небезопасных для безопасности станции условий может повлиять на правильность принятия решений оператора. И, наконец, оператор может совершить ошибку на этапе ввода управляющих команд.

С точки зрения теории контроля будем учитывать следующие типы ошибок оператора:

– ошибки 1 – го рода (оператор посредством ЧМИ идентифицирует систему, как отказавшую, несмотря на ее работоспособное состояние);

– ошибки 2 – го рода (оператор посредством ЧМИ идентифицирует систему как работоспособную в ситуации ее отказа);

– ошибки 3 – го рода (оператор посредством ЧМИ не получает информацию об отказе).

Разработка модели готовности ИУС с учетом ЧМИ

Исходя из вышесказанного, можно построить граф состояний информационной системы без управления функционированием, представленный на рис. 2.

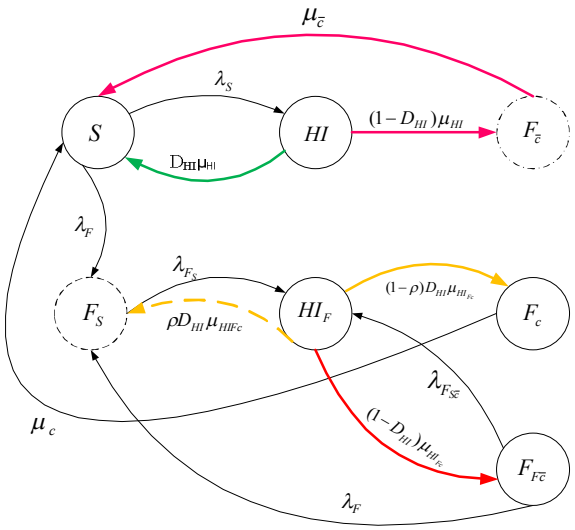

Рис. 2. Размеченный граф состояний информационной системы без управления функционированием - М1

В общем случае система может находиться в одном следующих состояний:

S - исправное состояние системы;

HI - состояние реакции оператора на воспринимаемую информацию, отображаемую ЧМИ, при работоспособном состоянии системы;

$F_{\bar{c}}$ - состояние ложного отказа системы (оператор ошибочно диагностировал отказ исправной системы);

F_s - состояние отказа в системе;

HI_F - состояние ЧМИ при отказе системы;

F_c - состояние верного отказа (оператор правильно диагностировал отказ системы);

$F_{F_{\bar{c}}}$ - состояние скрытого отказа (оператор не смог обнаружить отказ системы);

λ_s - интенсивность потока обращений к оператору (HI);

μ_{HI} - интенсивность потока реакций от оператора (HI);

λ_{Fs} - интенсивность потока обращений к интерфейсу при отказе системы;

$\mu_{\bar{c}}$ - интенсивность потока восстановления при отказе $F_{\bar{c}}$;

D_{HI} - вероятность правильных действий (реакций) оператора;

μ_c - интенсивность восстановления системы при отказе F_c ;

λ_F - интенсивность потока отказов системы;

$\lambda_{F_{S\bar{c}}}$ - интенсивность потока обращений к оператору (ЧМИ) при скрытом отказе;

$\mu_{HI_{Fc}}$ - интенсивность потока реакций оператора при отказе системы;

ρ - метрика (меняется в пределах от 0 до 1) учета необходимости дополнительного запроса при отказе объекта.

Логика функционирования состоит в следующем. В начальный момент времени t_0 система реализует все предписанные функции и находится в состоянии S. Процесс корректного взаимодействия оператора и ИУС посредством использования ЧМИ описан переходом из состояния S в состояние HI с интенсивностью λ_s и возвращением из HI в S с интенсивностью $D_{HI}\mu_{HI}$ в случае правильных действий оператора. В случае, если оператор проводит неверное диагностирование исправной ИУС, ошибочно предполагая возникновение отказа (ошибка 1-го рода), система переходит в состояние $F_{\bar{c}}$ с интенсивностью $(1-D_{HI})\mu_{HI}$ и восстанавливается с интенсивностью $\mu_{\bar{c}}$. В случайный момент времени t_n появляется отказ ИУС и система переходит из состояния S в F_S с интенсивностью λ_F. Процесс передачи потока сигналов неисправной ИУС, отображенного с помощью ЧМИ, описывается переходом из состояния F_s в HI_F и определяется значением λ_{F_s}. Корректное восприятие оператором информации о возникшем отказе и попытка проведения диагностирования отказа системы определяется возвращением из состояния HI_F в F_s с интенсивностью восстановления $\rho D_{HI}\mu_{HI_F}$. В том случае, если оператор верно диагностировал отказ ИУС, система переходит из HI_F в F_c с интенсивностью $(1-\rho)D_{HI}\mu_{HI_{F_c}}$ и при устранении отказа восстанавливается в работоспособное состояние S с интенсивностью μ_c. Если же произошел скрытый отказ, (ошибка 3-го рода) и таким образом, оператор не предпринял никаких действий по его устранению, система переходит из состояния HI_F в $F_{F_{\bar{c}}}$ с интенсивностью $(1-D_{HI})\mu_{HI_F}$. Процесс нахождения системы в состоянии скрытого отказа при нехватке оператору информации для корректного диагностирования ИУС, описывается переходом из $F_{F_{\bar{c}}}$ в HI_F со значением $\lambda_{F_{F_{\bar{c}}}}$. В данном случае ИУС продолжает находиться в состоянии отказа, что определяется переходом из $F_{F_{\bar{c}}}$ в F_s с интенсивностью λ_F.

На рис. 3 приведен марковский граф ИУС с управлением функционирования. Этот граф содержит то же множество состояний, что и предыдущий, но имеет дополнительные переходы, которые показывают, что оператор может управлять ИУС. Кроме того, здесь используются дополнительные параметры:

α – метрика (меняется в пределах от 0 до 1) возможности выполнения корректирующих действий;

ω_i – вероятность различных ошибок оператора (ω_0 – перевода системы в состояние явного отказа; ω_1 – перевода системы в состояние ложного отказа; ω_2 – перевода системы в состояние скрытого отказа); $\sum_{i=0}^{2}\omega_i = 1$.

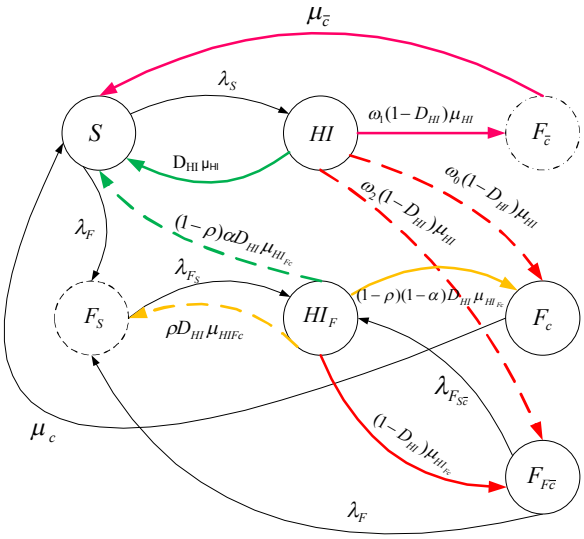

Рис. 3. Граф состояний информационно-управляющей системы с управлением функционированием - М2

Логика функционирования данной системы практически идентична с системой рассмотренной выше. Опишем дополнительные переходы, определяющие возможность оператора управлять системой. В начальный момент времени t_0 система реализует все предписанные функции и находится в состоянии *S*. Процесс корректного взаимодействия оператора и ИУС посредством использования ЧМИ, описан переходом из состояния *S* в состояние *HI* с интенсивностью λ_s, и возвращением из *HI* в *S* с интенсивностью $D_{HI}\mu_{HI}$ в случае верных действий оператора, и является идентичным с системой без управления функционированием. В том случае, когда оператор выполнил некорректные действия и перевел исправную систему в состояние ложного отказа система переходит из состояния *HI* в состояние $F_{\bar{c}}$ с интенсивностью $\omega_1(1-D_{HI})\mu_{HI}$ Если же оператор выполнил действия и перевел исправную систему в состояние явного отказа система переходит из состояния *HI* в состояние F_C с интенсивностью $\omega_0(1-D_{HI})\mu_{HI}$ В случае если оператор неверными действиями перевел исправную систему в состояние скрытого отказа система переходит из со-

стояния HI в состояние $F_{\overline{F_C}}$ с интенсивностью $\omega_2(1-D_{HI})\mu_{HI}$. Переход из состояния HI_F в S с интенсивностью $(1-\rho)\alpha D_{HI}\mu_{HI_{F_c}}$ происходит в случае если оператор выполняет верные действия в случае возникновения отказа системы и переводит ее в исправное состояние. Переход из HI_F в F_C с интенсивностью $(1-\rho)(1-\alpha)D_{HI}\mu_{HI_{F_c}}$ происходит в том случае, если при проявлении отказа оператор не выполняет корректирующих действий и таким образом переводит неисправную систему в состояние явного отказа.

Исследование марковской модели

В рамках данной работы была исследована модель готовности ИУС без управления функционированием. На основе марковской цепи М1 была построена система дифференциальных уравнений Колмогорова (1). Для решения системы дифференциальных уравнений был использован пакет компьютерной математики Mathematica.

$$
\begin{aligned}
&dP_S(t)/dt = -(\lambda_S+\lambda_F)P_S(t)+\mu_{\overline{C}}P_{F_{\overline{C}}}(t)+\mu_C P_{F_C}(t)+D_{HI}\mu_{HI}P_{HI}(t);\\
&dP_{HI}(t)/dt = -(D_{HI}\mu_{HI}+(1-D_{HI})\mu_{HI})P_{HI}(t)+\lambda_S P_S(t);\\
&dP_{F_{\overline{C}}}(t)/dt = -\mu_{\overline{C}}P_{F_{\overline{C}}}(t)+(1-D_{HI})\mu_{HI}P_{HI}(t);\\
&dP_{F_S}(t)/dt = -\lambda_{F_S}P_{F_S}(t)+\lambda_F P_S(t)+\lambda_F P_{F_{\overline{C}}}(t)+\rho D_{HI}\mu_{HIF_C}P_{HI_F}(t);\\
&dP_{HI_F}(t)/dt = -(\rho D_{HI}\mu_{HIF_C}+(1-D_{HI})\mu_{HIF_C}+(1-\rho)D_{HI}\mu_{HIF_C})P_{HI_F}(t)+\lambda_{F_S}P_{F_S}(t)+\lambda_{F_{S_{\overline{C}}}}P_{F_{S_{\overline{C}}}}(t);\\
&dP_{F_C}(t)/dt = -\mu_C P_{F_C}(t)+(1-\rho)D_{HI}\mu_{HIF_C}P_{HI_F}(t);\\
&dP_{F_{\overline{F_C}}}(t)/dt = -(\lambda_F+\lambda_{F_{S_{\overline{C}}}})P_{F_{\overline{F_C}}}(t)+(1-D_{HI})\mu_{HIF_C}.
\end{aligned}
\qquad (1)
$$

Значения параметров могут быть получены на основе анализа документации, данных о результатах эксплуатации и экспертных оценок. Задача параметризации модели является отдельной задачей, которая в данной статье не рассматривается. Для тестирования модели использовались следующие значения параметров: $\lambda_s = 0{,}3*10^4$ 1/ч; $\mu_{HI} = 0{,}2*10^4$ 1/ч; $\lambda_{F_s} = \varepsilon\lambda_s, \varepsilon > 1$ при $\varepsilon = 10, \lambda_{F_S} = 0{,}3*10^5$ 1/ч; $\mu_{HI_{F_c}} = \chi\mu_{HI}$ при $\chi = 1$, $\mu_{HI_{F_C}} = 0{,}2*10^4$ 1/ч;

$D_{HI} = 0{,}9$; $\rho = 0{,}1$; $\lambda_{F_{S_{\overline{c}}}} \cong \lambda_{F_S} = 2{,}8*10^4$ 1/ч;

$\lambda_F = 10^{-2}$ 1/ч; $\mu_{\overline{c}} = 0{,}1$ 1/ч; $\mu_c = 0{,}001$ 1/ч для случая $\mu_{\overline{c}} = 10^{-2}$ 1/ч; $\mu_{\overline{c}} = \mu_c * \theta$, $\theta > 1$, $\theta = 10$;

$\alpha = 0{,}1$; $\omega_0 = 0{,}05$; $\omega_1 = 0{,}45$; $\omega_2 = 0{,}5$.

Используя данную систему дифференциальных уравнений, вычисляем значения вероятностей нахождения системы во всех возможных состояниях

$$\left\{S, HI, F_{\overline{c}}, F_s, HI_F, F_c, F_{\overline{F_c}}\right\}$$

в момент времени t_i,

i =1,…,n, где n=50, $t \in [0;9800]$ ч., Дt = 200 ч.

Для тестовых значений параметров имеем следующий результат (рис. 4). При исследовании ИУС для модели М1 получены численные результаты, которые приведены в табл. 1.

A(t), которая вычисляется для исследования системы (рис. 2, 3), как A(t) = S(t) + HI(t). График функции готовности, представленной на рис. 2, изображен на рис. 4. Шкала времени для построения графика выбрана продолжительностью 9800 часов.

Таблица 1

Значения вероятностей состояний для модели М1

Время (час)	**Вероятности состояний ИУС**						
	S	HI	$F_{\overline{c}}$	F_S	HI_F	F_C	$F_{\overline{F_C}}$
0	1	0	0	0	0	0	0
200	0,916961	0,0829277	0,000111191	$2{,}4913*10^{-7}$	$2{,}54135*10^{-8}$	$5{,}46844*10^{-9}$	$1{,}20048*10^{-10}$
400	0,844943	0,154375	0,000680831	$2{,}89548*10^{-7}$	$2{,}27798*10^{-7}$	$1{,}96107*10^{-9}$	$3{,}22269*10^{-10}$
600	0,782461	0,215893	0,00164539	$2{,}825*10^{-7}$	$4{,}20169*10^{-7}$	$7{,}04419*10^{-8}$	$1{,}37879*10^{-9}$
800	0,728228	0,268821	0,00294991	$2{,}66172*10^{-7}$	$5{,}70241*10^{-7}$	$1{,}55363*10^{-7}$	$2{,}62665*10^{-9}$
1000	0,681133	0,314319	0,00454685	$2{,}4943*10^{-7}$	$6{,}79489*10^{-7}$	$2{,}66658*10^{-7}$	$3{,}72091*10^{-9}$
…							
9000	0,33794	0,537753	0,124301	$1{,}16375*10^{-7}$	$5{,}31544*10^{-7}$	$5{,}28613*10^{-6}$	$3{,}82138*10^{-9}$
9200	0,336638	0,535988	0,127368	$1{,}15915*10^{-7}$	$5{,}28962*10^{-7}$	$5{,}38564*10^{-6}$	$3{,}80187*10^{-9}$
9400	0,335356	0,534213	0,130424	$1{,}15464*10^{-7}$	$5{,}2648*10^{-7}$	$5{,}48466*10^{-6}$	$3{,}78319*10^{-9}$
9600	0,334099	0,53243	0,133471	$1{,}1502*10^{-7}$	$5{,}24086*10^{-7}$	$5{,}58323*10^{-6}$	$3,\ 76525*10^{-9}$
9800	0,332846	0,530641	0,136507	$1{,}14583*10^{-7}$	$5{,}2177*10^{-7}$	$5{,}68135*10^{-6}$	$3{,}74797*10^{-9}$

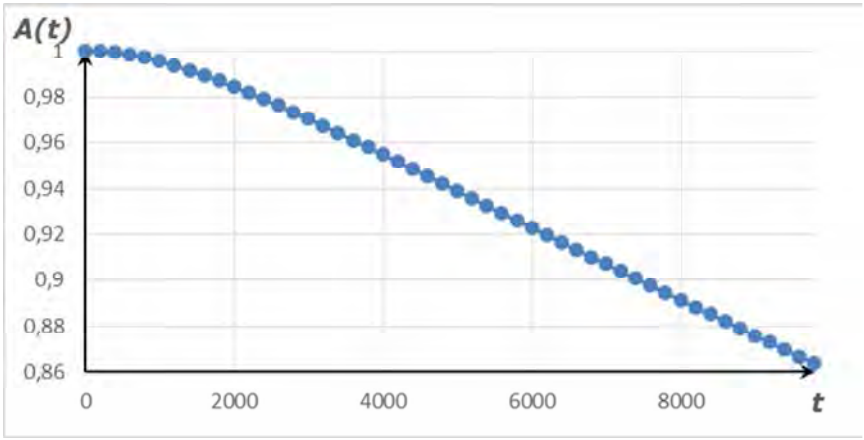

Рис. 4. График функции готовности ИУС без управления функционированием

Стационарный режим при данных значениях параметров для ИУС не наступает в течение рассматриваемого промежутка времени. Это может быть объяснено тем, что функция готовности принимает установившееся значение позже и готовность системы не является высокой из-за малой надежности ЧМИ (параметры $D_{HI}, \mu_{HI_{F_c}}, \lambda_{F_{S_{\bar{c}}}}$).

Заключение

Полученные в данной работе результаты тестовых исследований позволяют сделать вывод о возможности построения адекватных и более детальных, чем известные, марковских моделей, которые позволяют описывать состояния ИУС с учетом различных последствий ошибочных действий оператора и дефектов ЧМИ. Дальнейшие исследования могут быть направлены на решение задачи параметризации модели и получения развернутых оценок готовности ИУС с учетом человеческого фактора и качества ЧМИ.

Список литературы

1. Вентцель Е.С. Исследование операций / Е.С. Вентцель. – М.: Радио и связь, 1972. – 368 с.

2. Информационные технологии для критических инфраструктур: монография [Текст] / Под ред. А.В. Скаткова // – Севастополь: СевНТУ. – 2012. – 306 с.

3. Earl Smith, W. Availability analysis of multi-component blade server systems / W. Earl Smith, K. S. Trivedi, L. Tomek, J. Ackeret. // Allen Press, Inc. IBM Systems Journal. – 2008. – Vol. 47, №4. – P. 1 – 20.

4. Andrew Rae Helping the operator in the loop: practical human machine interface principles for safe computer controlled systems [Text] / Andrew Rae // Proceeding SCS '07 Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems. – 2007. – Vol. 86. – P. 61-70

5. Thimbleby H. Usability analysis with Markov models / Thimbleby H., Cairns P., Jones M. // ACM Transactions on Computer-Human Interaction – 2001. – Vol. 8, № 2. – P. 99 – 132.

6. Smolarek L. Finite discrete Markov model of ship safety [Text] / L. Smolarek // TransNav, International journal on marine navigation and safety of sea transportation. – 2010. – Vol. 4, №2. – P. 223 – 226.

7. Гумиров Ш.Ш. Метод адаптации пользовательского интерфейса телекоммуникационных сервисов на основе скрытых Марковских моделей / Ш.Ш. Гумиров // Вестник НГУ. Серия: Информационные технологии. – 2010. – Т. 8, № 2. – С. 43 – 53.

8. Полетыкин А.Г. Исследование и разработка методов и программных средств для информационно-управляющих систем верхнего блочного уровня АСУ ТП АЭС / А.Г. Полетыкин. – М.: Институт проблем управления им. В. А. Трапезникова РАН, автор. дисс, – 2007, – 41 с.

Поступила в редколлегию 22.01.2013

Рецензент: д-р техн. наук проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

РОЗРОБКА МАРКІВСЬКИХ МОДЕЛЕЙ ГОТОВНОСТІ ІНФОРМАЦІЙНИХ І КЕРУЮЧИХ СИСТЕМ З УРАХУВАННЯМ ХАРАКТЕРИСТИК ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ

А.О. Орєхова, В.С. Харченко, Є.В. Брежнєв, В.О. Бутенко

Аналізується клас інформаційно-керуючих систем, в яких помилки оператора або дефекти людино-машинного інтерфейсу можуть призвести до переходу системи в стан безпечної та небезпечної відмов. Запропоновано марковські моделі готовності інформаційних і керуючих систем, які враховують характеристики людино-машинного інтерфейсу і помилки оператора. Наводяться точкові результати дослідження марковських моделей готовності за допомогою пакету програм Mathematica.

***Ключові слова**: інформаційно-керуючі системи, людино-машинний інтерфейс, марківські моделі, готовність.*

DEVELOPMENT OF MARKOV MODELS OF PREPAREDNESS OF THE INFORMATION AND CONTROL SYSTEMS TAKING INTO ACCOUNT CHARACTERISTICS OF HMI.

A.A. Orekhova, V.S. Kharchenko, E.V. Brezhnev, V.O. Butenko

Object of analysis is type of the information and control system, which can go to safe or dangerous failure state because of operator or HMI errors. Are used Avaliability Markov's Models which allow consider HMI characteristics and possibility of user errors. Results of research obtained with using package programms Mathematica.

***Keywords**: management, human-machine interface, Markov models, availability, information and control system.*