УДК 004.052.2

В.В. СКЛЯР

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

АНАЛИЗ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ЛОГИЧЕСКИХ МОДЕЛЕЙ ОШИБОК КОНТРОЛЯ И УПРАВЛЕНИЯ

Устойчивость к отказам программно-аппаратных средств является важной составляющей функциональной безопасности информационно-управляющих систем (ИУС), а также других критических характеристик систем, важных для безопасности (гарантоспособности, способность к эволюции и т.п.). В статье рассмотрены логические модели ошибок контроля и управления I, II и III рода с учетом их влияния на безопасность системы. Дальнейшим направлением исследования может выступать разработка марковских и полумарковских моделей ИУС с учетом ошибок контроля и управления I, II и III рода с дальнейшим определением численных показателей надежности и безопасности.

Ключевые слова: *отказоустойчивость, ошибки контроля и управления, ошибки I и II рода.*

Введение

Термин «обнаружение ошибок» первоначально возник в теории информации и связи, и применяется он для обозначения действий, направленных на контроль целостности данных при записи, воспроизведении или передаче информации [1]. Под коррекцией ошибок подразумевается процедура восстановления информации после чтения ее из устройства хранения или канала связи. В теории надежности и технической диагностике [2] способность системы к обнаружению и коррекции ошибок контроля и управления является важной составляющей отказоустойчивости. В работе [3] рассмотрены свойства эволюционирующих систем, в том числе, и отказоустойчивость. В работе [4] предложены базовые модели для оценки влияния ошибок контроля и управления на безопасность информационно-управляющих систем.

На данный момент важным направлением является развитие математического аппарата оценки функциональной безопасности ИУС [5].

Целью настоящей статьи является разработка логических моделей контроля и управления ИУС, учитывающих влияние ошибок контроля и управления I, II и III рода на безопасность системы.

1. Ошибки контроля и управления I и II рода

Рассмотрим логику выполнение функций ИУС, которая, с одной стороны, предназначена для функционирования совместно с объектом контроля и управления (ОКУ), а с другой стороны, включает устройство контроля (УК) и устройства управления (УУ) (рис. 1) [4].

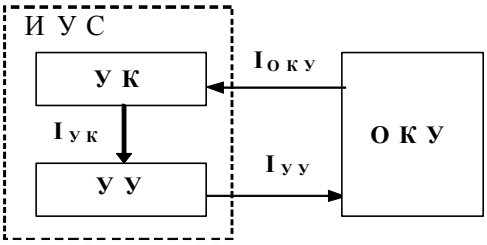

Рис. 1. Взаимодействие объекта контроля и управления с устройствами контроля и управления в составе ИУС

Для примера проанализируем выполнение функций контроля и управления для такого ОКУ, для которого требуется распознание безопасного состояния ($\overline{\mathrm{O}}$) и опасного состояния (О). Тогда множество состояний ОКУ включает $\mathrm{MS}^{\mathrm{OKY}} = \left\{\overline{\mathrm{O}}, \mathrm{O}\right\}$ (см. рис. 2).

УК может, как безошибочно распознавать состояние ОКУ, так и допускать ошибки первого и второго рода. Под ошибками контроля I рода понимается такая ситуация, когда при нахождении ОКУ в безопасном состоянии УК определяет его состояние как опасное («ложное срабатывание»). Под ошибками контроля II рода понимается такая ситуация, когда при нахождении ОКУ в опасном состоянии УК определяет его состояние как безопасное («ложное несрабатывание»).

Тогда множество состояний УК (с точки зрения распознания состояний ОКУ) включает $\mathrm{M}\overline{\mathrm{S}}^{\mathrm{YK}} = \left\{\overline{\mathrm{O}}\,\overline{\mathrm{O}}, \overline{\mathrm{O}}\mathrm{O}, \mathrm{OO}, \mathrm{O}\overline{\mathrm{O}}\right\}$, где $\overline{\mathrm{O}}\,\overline{\mathrm{O}}$ – правильно распознанное безопасное состояние, $\overline{\mathrm{O}}\mathrm{O}$ – ошибка контроля I рода, OO – правильно распознанное опасное состояние, $\mathrm{O}\overline{\mathrm{O}}$ – ошибка контроля II рода.

Опасными состояниями УК являются ошибки II рода, поскольку в этом случае будут отсутствовать действия по переводу ОКУ в безопасное состояние, что может привести к катастрофическим последствиям.

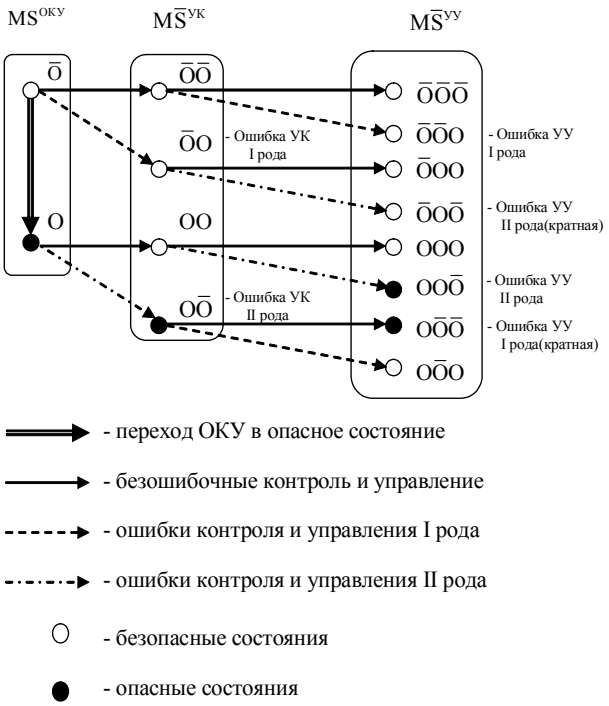

Рис. 2. Общий вид логической модели ошибок контроля и управления ИУС

Ошибки I и II рода может также допускать УУ. Ошибки управления I рода заключаются в выдаче управляющих воздействий, соответствующих опасному состоянию ОКУ, при определении УК состояния ОКУ как безопасного (как правило, такие управляющие воздействия заключаются в переводе ОКУ в безопасное состояние). Ошибки управления II рода заключаются в отсутствии управляющих воздействий, соответствующих опасному состоянию ОКУ, при определении УК состояния ОКУ как опасного. С учетом суперпозиции ошибок контроля, и управления, могут существовать кратные ошибки, однако вероятность их крайне мала, поскольку определяется произведением вероятностей возникновения ошибок.

Тогда множество состояний УУ (с точки зрения выдачи управляющих воздействий на основании информации $M\overline{S}^{УК}$, полученной от УК) включает

$$M\overline{S}^{УУ}=\left\{\begin{matrix}\overline{O}\,\overline{O}\,\overline{O},\overline{O}\,\overline{O}O,\overline{O}OO,\overline{O}O\overline{O},\\ OOO,OO\overline{O},O\overline{O}\,\overline{O},O\overline{O}O\end{matrix}\right\},$$

где $\overline{O}\,\overline{O}\,\overline{O}$ – правильное управление при правильно распознанном безопасном состоянии, $\overline{O}\,\overline{O}O$ – ошибка управления I рода при правильно распознанном безопасном состоянии, $\overline{O}OO$ – правильное управление при ошибке контроля I рода, $\overline{O}O\overline{O}$ – ошибка управления II рода при ошибке контроля I рода, OOO – правильное управление при правильно распознанном опасном состоянии, $OO\overline{O}$ – ошибка управления II рода при правильно распознанном опасном состоянии, $O\overline{O}\,\overline{O}$ – правильное управление при ошибке контроля II рода; $O\overline{O}O$ – ошибка управления I рода при ошибке контроля II рода.

Опасными состояниями УУ являются ошибки управления II рода при правильно распознанном опасном состоянии ($OO\overline{O}$), а также правильное управление при ошибке контроля II рода ($O\overline{O}\,\overline{O}$).

2. Ошибки контроля и управления III рода

Рассмотрим так называемые ошибки III рода, которые могут дополнительно иметь место в случае, когда состояния ОКУ описываются моделью

$$MS=\Big\{S_{И},\ MS_{НИР}=\bigcup_{a=1}^{c_{НИР}}S_{НИРi},\ MS_{ЧР}=\bigcup_{b=1}^{c_{ЧР}}S_{ЧРj},\ MS_{НРБ}=\bigcup_{c=1}^{c_{НРБ}}S_{НРБk},\ MS_{НРО}=\bigcup_{d=1}^{c_{НРО}}S_{НРОm}\Big\},\quad(1)$$

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 справедливо $S_{ni}\bigcap S_{nj}=\varnothing$, где $n_i\in N$, $n_j\in N$ – индексы двух различных множеств состояний; $N=\{И,НИР,ЧР,НРБ,НРО\}$ – множество типов состояний;

$c_{НИР}$, $c_{ЧР}$, $c_{НРБ}$, $c_{НРО}$ – мощности соответствующих множеств.

Ошибки III рода обусловлены наличием подмножеств состояний $MS_{НИР}$, $MS_{ЧР}$, $MS_{НРБ}$, $MS_{НРО}$. При ошибках контроля и управления III рода правильно определяется тип (подмножество состояния), однако неправильно определяется состояние в рамках подмножества (см. рис. 3). В этом случае ошибки контроля и управления нельзя отнести ни к I, ни ко II роду, поскольку невозможно идентифицировать подобное событие ни как «ложное срабатывание», ни как «ложное несрабатывание».

Следует отметить, что состояния $M\overline{S}^{УК}$ фактически представляют собой состояния ОКУ с учетом определения его состояния посредством УК. Аналогично, состояния $M\overline{S}^{УУ}$ представляют собой состояния ОКУ с учетом определения его состояния посредством УК и с учетом воздействия, сформиро-

ванного УУ на основании информации от УК. В этом состоит их отличие от состояний $MS^{УК}$, $MS^{УУ}$, описываемых моделью (1) и заключающихся в физической степени деградации УК и УУ.

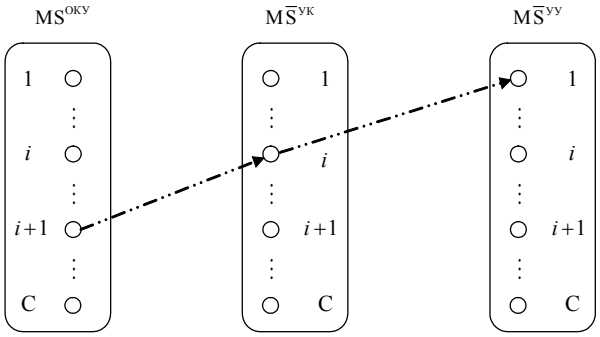

Рис. 3. Логическая модель ошибок контроля и управления III-го рода

3. Логические модели ошибок контроля и управления

Построим логические модели ошибок контроля и управления ИУС. Построим, для начала, логическую модель ошибок контроля, упростив ее отсутствием рассмотрения ошибок III рода (см. рис. 4).

При анализе модели, представленной на рис. 2, было отмечено, что ошибки контроля II рода могут приводить к возникновению как опасных, так и безопасных состояний. Будем называть ошибки контроля II рода, в результате которых возникает опасное состояние, ошибками контроля IIо рода. Введем также понятие потенциально опасного состояния. Потенциально опасным будем называть такое состояние, когда вследствие ошибки I рода состояние ОКУ распознается как опасное, и к нему применяются такие действия, которые создают риск для ОКУ, находящегося в безопасном состоянии (например, автоподрыв ракеты из-за ошибки контроля I рода). Ошибки контроля I рода, в результате которых возникает потенциально опасное состояние, будем называть контроля Iо рода.

Потенциально опасные состояния ОКУ возникают из-за ошибок контроля Iо рода, в результате которых безопасное состояние ОКУ ($S_{И}^{ОКУ} \vee MS_{НИР}^{ОКУ} \vee MS_{ЧР}^{ОКУ} \vee MS_{НРБ}^{ОКУ}$) идентифицируется УК, как неработоспособное опасное ($M\bar{S}_{НРО}^{УК}$). Опасные состояния ОКУ возникают из-за ошибок контроля IIо рода, в результате которых неработоспособное опасное состояние ОКУ ($MS_{НРО}^{ОКУ}$) идентифицируется УК, как безопасное ($\bar{S}_{И}^{УК} \vee M\bar{S}_{НИР}^{УК} \vee M\bar{S}_{ЧР}^{УК} \vee M\bar{S}_{НРБ}^{УК}$).

При анализе ошибок управления учтем ошибки III рода (см. рис. 5). Для этого необходимо дифференцировать состояния подмножеств $MS_{НИР}$, $MS_{НРБ}$, $MS_{НРО}$. Среди ошибок контроля III рода могут быть выделены ошибки IIIо рода, в результате которых возникает опасное состояние. К ошибкам контроля IIIо рода относятся ошибки в идентификации состояний ОКУ из множества неработоспособных опасных ($MS_{НРО}^{ОКУ}$).

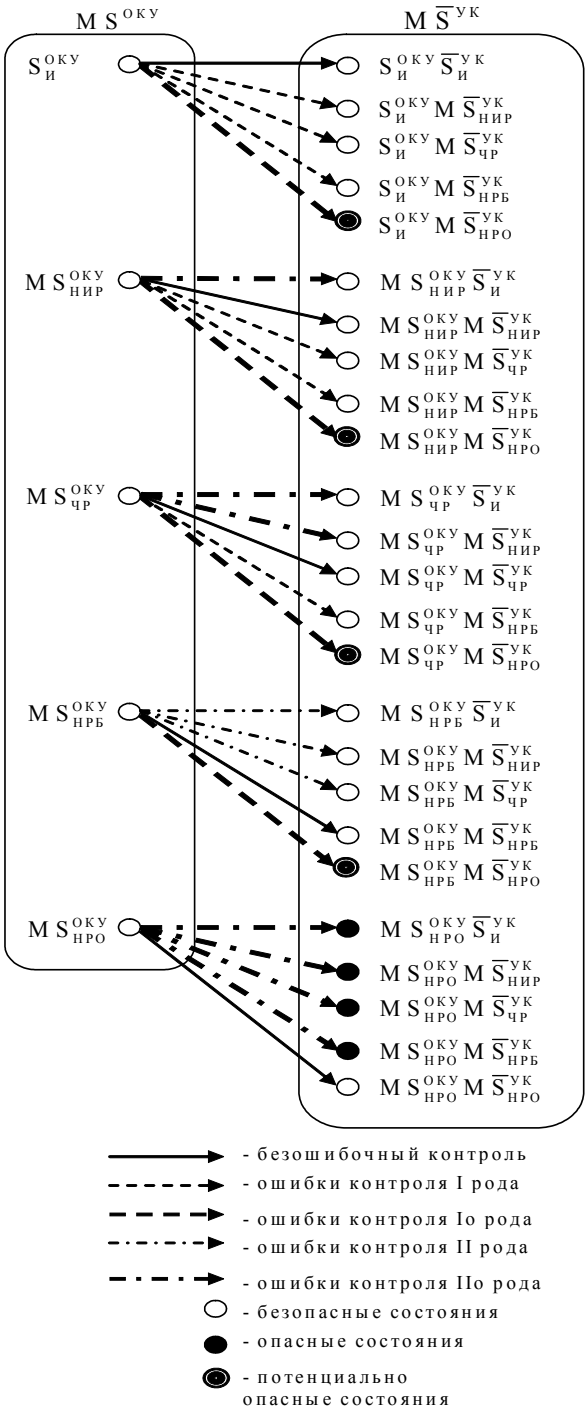

Рис. 4. Логическая модель ошибок контроля ИУС без учета ошибок III рода

Чтобы не увеличивать количество комбинаций таких логических моделей ошибок управления, в

качестве отправной точки можно рассматривать состояния ОКУ с учетом результатов работы УК, без рассмотрения предшествующих ошибок контроля. Ошибки управления I, Io, II, IIo III и IIIo рода по своему физическому смыслу аналогичны подобным ошибкам контроля. Условия возникновения потенциально опасных и опасных состояний в случае ошибок управления также аналогичны подобным ситуациям в случае ошибок контроля.

Отличие моделей ошибок контроля и моделей ошибок управления заключается в том, что управляющие воздействия УУ одинаковы для исправного состояния ($\overline{S}_{И}^{УУ}$) и для неисправных работоспособных состояний ($M\overline{S}_{НИР}^{УУ}$). По этой причине на рис. 5 введены общие состояния $\overline{S}_{И}^{УУ}(M\overline{S}_{НИР}^{УУ})$.

4. Эшелоны защиты технических комплексов

Суть принципа глубокоэшелонированной защиты [6] заключается в специальном распределении по уровням всех действий, оборудования и процедур, направленных на обеспечение безопасности ОКУ. Распределение по уровням осуществляется таким образом, чтобы на каждом из уровней, во-первых, обеспечивалось предупреждение возникновения событий, способных повлечь необходимость в следующем уровне защиты, и, во-вторых, ограничивались последствия, возникшие в результате нарушений в предыдущем уровне защиты.

С точки зрения безопасности может быть выделено два типа ИУС. Первый тип включает ИУС, предназначенные для контроля и управления активами в режиме нормальной эксплуатации (системы нормальной эксплуатации – СНЭ). Данные ИУС являются частью активов и увеличивают риски активов за счет собственных внутренних рисков. Второй тип включает ИУС, предназначенные для контроля и управления активами в экстренных (аварийных) режимах (системы безопасности – СБ). Данные ИУС снижают риски активов до уровня собственных внутренних рисков.

Таким образом, первый эшелон защиты включает СНЭ, которые обеспечивают безопасную эксплуатацию активов в штатных режимах. Если происходит событие, нарушающее нормальную эксплуатацию активов, подключается второй эшелон защиты, включающий СБ. Функции СБ заключаются в прекращении эксплуатации активов и в переводе активов в безопасное неработоспособное состояние. Отметим, что в зависимости от видов активов эшелон СБ может включать несколько подэшелонов защиты.

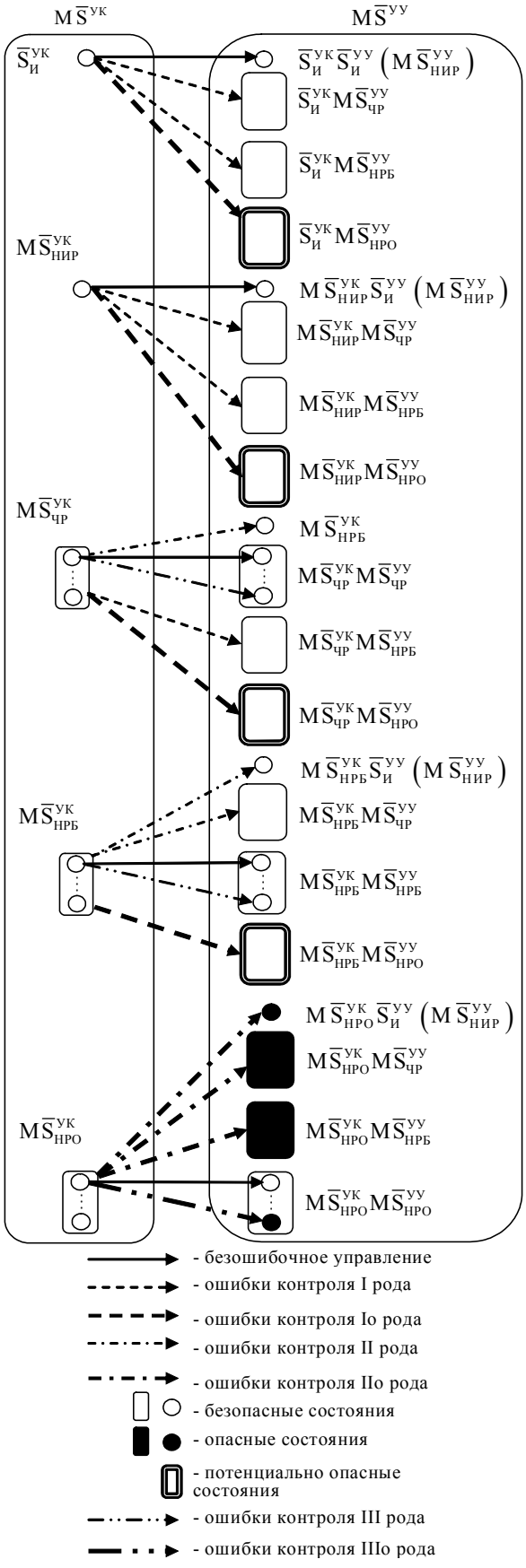

Рис. 5. Логическая модель ошибок управления ИУС с учетом ошибок III рода

Таким образом, логические модели ошибок контроля и управления ИУС могут быть дифференцированы с учетом специфики СНЭ и СБ. Основное отличие СНЭ и СБ заключается в форме модели состояний. СНЭ описываются моделью состояний (1), следовательно, для таких систем логические модели ошибок контроля и управления будут соответствовать рис. 4 и 5. СБ отличается тем, что для нее частично работоспособные состояния эквивалентны неработоспособным безопасным состояниям, т.е.

$$MS=\left\{S_{и}, MS_{НИР}=\bigcup_{a=1}^{c_{НИР}} S_{НИРi}, MS_{НРБ}=\bigcup_{c=1}^{c_{НРБ}} S_{НРБк}, MS_{НРО}=\bigcup_{d=1}^{c_{НРО}} S_{НРОm}\right\}. \quad (3)$$

Таким образом, логические модели ошибок контроля и управления для СБ будут иметь более простой вид за счет отсутствия частично работоспособных состояний.

Заключение

В статье рассмотрены логические модели ошибок контроля и управления I, II и III рода с учетом их влияния на безопасность системы.

Дальнейшим направлением исследования может выступать разработка марковских и полумарковских моделей ИУС с учетом ошибок контроля и управления I, II и III рода с дальнейшим определением численных показателей надежности и безопасности.

Литература

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса – М.: Техносфера, 2005. – 320 с.

2. Глущенко П.В. Техническая диагностика / П.В. Глущенко – М.: Вузовская книга, 2004. – 248 с.

3. Харченко В.С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2009. – № 7. – С. 46-59.

4. Харченко В.С. Теоретико-множественные модели состояний отказоустойчивых информационно-управляющих систем с учетом их влияния на безопасность / В.С. Харченко, В.В Скляр, А.Х. Аль-Тарази // Радіоелектронні і комп'ютерні системи. – 2004. – № 2. – С. 67-74.

5. Федоров Ю.Н. Справочник инженера по АСУ ТП: Проектирование и разработка / Ю.Н. Федоров – М.: Инфра-Инженерия, 2008. – 928 с.

6. Скляр В.В. Оценка качества и экспертизы программного обеспечения. Лекционный материал / Скляр В.В.; под. ред. Харченко В.С. – Харьков: Нац. аэрокосмический ун-т «Харьк. авиац. ин-т», 2008. – 204 с.

Поступила в редакцию 20.01.2009

Рецензент: д-р техн. наук, проф., проф. кафедры В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.

АНАЛІЗ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ З ВИКОРИСТАННЯМ ЛОГІЧНИХ МОДЕЛЕЙ ПОМИЛОК КОНТРОЛЮ ТА УПРАВЛІННЯ

В.В. Скляр

Стійкість до відмов програмно-апаратних засобів є важливою складовою функціональної безпеки інформаційно-управляючих систем (ІУС), а також інших критичних характеристик систем, важливих для безпеки (гарантоспособности, здатність до еволюції й т.п.). У статті розглянуті логічні моделі помилок контролю й керування I, II й III роду з урахуванням їх впливу на безпеку системи.

Ключові слова: відмовостійкість, помилки контролю та управління, помилки I та II роду.

FUNCTIONAL SAFETY ANALYSIS OF INSTRUMENTATION AND CONTROL SYSTEMS BY USE OF LOGICAL MODELS CHECKING AND CONTROL ERRORS

V.V. Sklyar

Resilience to software and hardware failures is an important part of instrumentation and control systems functional safety and another systems safety critical characteristics (dependability, evolvability etc.) Logical models of alpha, beta and gamma checking and control errors taking into account systems safety influence are regarded in this paper.

Key words: fault-tolerance**,** checking and control errors, alpha and beta errors.

Скляр Владимир Владимирович – канд. техн. наук, доц., доц. кафедры технологии компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: vvsklyar@mail.ru.