УДК 629.039.58

В. В. СКЛЯР[1], О. Н. ОДАРУЩЕНКО[1], Ю. Л. ПОНОЧОВНЫЙ[2], Е. Н. БУЛЬБА[1], А. О. ИВАСЮК[1]

[1] ***«Научно-производственное предприятие «Радий», Кировоград, Украина***
[2] ***Полтавский национальный технический университет им. Ю. Кондратюка, Украина***

МОДЕЛИ ОТКАЗОВ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ОСНОВЕ САМОДИАГНОСТИРУЕМЫХ ПРОГРАММИРУЕМЫХ ПЛАТФОРМ В СИСТЕМАХ АВАРИЙНОЙ ЗАЩИТЫ РЕАКТОРОВ

В статье рассмотрены особенности построения и функционирования системы аварийной защиты реакторов и ее ядра – информационно-управляющей системы (ИУС) на основе самодиагностируемой программируемой платформы. Выделены основные компоненты ИУС, позволяющие проводить диагностирование и выявление отказов в режиме реального времени. Приведена базовая марковская модель функционирования ИУС, учитывающая проявление обнаруженных и необнаруженных отказов и проведение периодических профилактик. Рассмотрена структурная схема надежности ИУС в режиме нормальной эксплуатации.

Ключевые слова: *информационно-управляющая система, функциональная безопасность, система аварийной защиты реакторов, самодиагностируемая программируемая платформа.*

Введение

При сертификации и оценке качества информационно-управляющих систем (ИУС) критических объектов, которые сами по себе опасности не несут, а лишь выполняют функции, важные для безопасности, рассматривается свойство функциональной безопасности.

Функциональная безопасность (ФБ) – часть безопасности, относящаяся к управляемому оборудованию и управляющей системе, которая зависит от правильного функционирования электрических, электронных и программируемых электронных систем, связанных с безопасностью технологических систем и оборудования для снижения внешнего риска [1]. Понятие функциональной безопасности включает в себя функции безопасности и целостность (интегрированность) безопасности.

Базовый стандарт по функциональной безопасности ISO/IEC 61508 рассматривает весь жизненный цикл электрических, электронных или программируемых электронных (E/E/PE) систем и изделий [1].

Принципы анализа функциональной безопасности изложены в [2]. Соблюдение всех требований, правил и норм позволяет избежать не только человеческих жертв, но и минимизировать риски любых ситуаций, которые могут к этому привести. В ряде случаев безопасность достигается путем использования сразу нескольких систем защиты, среди которых механические, пневматические, электрические, программируемые, электронные.

Оценивание функциональной безопасности – это определение показателя уровня риска, связанного с опасностью. Его значение является композицией вероятности опасных ситуаций и тяжести всех последствий, которые могут возникнуть за время эксплуатации. Особое по значимости место занимает оценка функциональной безопасности для систем аварийной защиты (САЗ) реакторных установок.

Постановка задачи исследования

Учет видов отказов является наиболее важной и сложной частью анализа надежности и функциональной безопасности систем [1]. При выполнении анализа функциональной безопасности систем актуализируются вопросы достоверности и применимости исходных данных по отказам, обнаруженным и необнаруженным системой контроля и диагностики, и учета их неопределенности в моделях расчета. Сложность учета отказов ИУС системы аварийной защиты реакторов заключается в большом количестве и сложности модели резервирования элементов системы [3, 4].

Таким образом, актуальной является задача разработки моделей отказов ИУС на основе самодиагностируемых программируемых платформ (СДПП) для обеспечения соответствующего уровня функциональной безопасности САЗ.

1. Состав и особенности реализации систем аварийной защиты реакторов

Анализ функциональной безопасности системы аварийной защиты является обязательным при проектировании блока. САЗ реактора является одной из наиболее важных систем безопасности и от ее надежности во многом зависит безопасность реакторной установки в целом.

В установках с реакторами ВВЭР-1000 функции САЗ по нейтронным и теплотехническим параметрам осуществляются комплексно, с помощью различных технических средств со специальным программным обеспечением. В их состав входят [3]:

– аппаратура контроля нейтронного потока;

– система группового и индивидуального управления стержнями САЗ;

– аппаратура контроля плотности выделения энергии;

– аппаратура защиты по технологическим параметрам;

– комплекс электрооборудования;

– аппаратура отображения и протоколирования;

– аппаратура логической обработки защитных сигналов;

– аппаратура контроля вибрации внутрикорпусных устройств;

– аппаратура коррекции показаний о нейтронном потоке;

– аппаратура регулирования мощности;

– аппаратура размножения сигналов;

– аппаратура формирования аварийных команд.

Отказы в САЗ возникают под воздействием разнообразных факторов. Поскольку каждый фактор в свою очередь зависит от многих причин, то отказы элементов, входящих в состав системы, относятся, как правило, к случайным событиям, а время работы до возникновения отказов соответственно является случайной величиной.

Системы аварийной защиты могут быть реализованы на основе платформ с использованием программируемых логических интегральных схем (ПЛИС). Основное внимание в таких платформах должно быть уделено диагностированию опасных и безопасных отказов системы.

Моделирование ИУС с системой контроля и диагностики на основе СДПП предусматривает последовательное рассмотрение трех моделей [5]:

– модель платформы без отказов,

– модель отказов (дефектов как их причин),

– модель платформы с дефектами.

Анализ отказов выполняется методами сбора и исследования информации об отказах системы в целом, либо элементов системы. Большинство методов основывается на проведении опросов экспертов, применении численных методов, экспериментальных исследованиях, методах теории вероятности и математической статистики [6].

Результатом такого анализа может быть построение дерева отказов САЗ, а также марковской модели состояний системы.

2. Состав и основные функции системы контроля и диагностики

В настоящее время существует два основных способа построения цифровых ИУС – на базе микропроцессорных технологий и на базе ПЛИС. Согласно [7] реализация функций зашиты, блокировок, управления и регулирования на базе ПЛИС является наиболее эффективным средством для разработки ИУС, соответствующих требованиям государственных и международных нормативно-технических документов по безопасности [1, 3, 8]. Использование ПЛИС для ИУС позволяет на этапе проектирования изначально заложить алгоритмы для самодиагностирования, которые будут выполняться отдельной функциональной подсистемой, называемой системой контроля и диагностики (СКД).

В результате исследования модели платформы СКД на основе СДПП без отказов было установлено, что её составляющие (программно-аппаратные модули) и связи между ними могут быть представлены в виде структурной схемы, где в центре информационного обмена находятся логический (LM) и диагностический (DM) модули (рис.1).

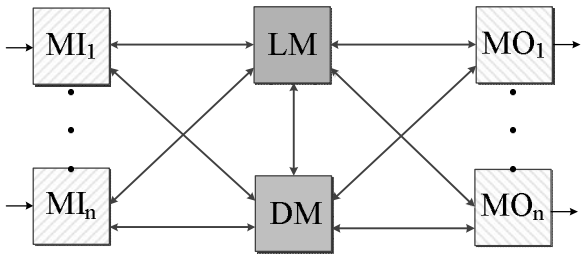

Рис. 1. Структурная модель системы контроля и диагностики на основе СДПП

Множество всех модулей ИУС представлено в следующем виде:

$$M = \{LM, DM, MI, MO\}, \quad (1)$$

где LM – логический модуль, DM – диагностический модуль, $MI=\{MI_1...MI_n\}$ – множество модулей входов, $MO=\{MO_1...MO_n\}$ – множество модулей выходов.

В предложенной модели СКД на основе СДПП самодиагностирование было разделено на три вида (рис. 2):

1. Встроенное аппаратное самодиагностирование (HW SD).

2. Программное самодиагностирование для интерфейсов передачи данных (IF SD).

3. Встроенное программное самодиагностирование для электронного проекта ПЛИС (ED SD).

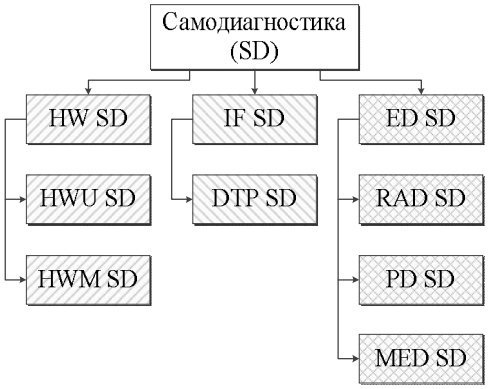

Рис. 2. Классификация видов самодиагностирования СКД на основе СДПП

Встроенное аппаратное самодиагностирование было поделено на два типа:

1. Встроенное аппаратное самодиагностирование на уровне узлов (HWU SD).

2. Встроенное аппаратное самодиагностирование на уровне модулей (HWM SD).

В свою очередь, программное самодиагностирование для интерфейсов включает в себя самодиагностирование для программных протоколов передачи данных (DTP SD). Встроенное программное самодиагностирование для электронного проекта ПЛИС включает в себя:

1. Самодиагностирование данных, хранящихся в ОЗУ ПЛИС (RAD SD).

2. Самодиагностирование пакетов данных (PD SD).

3. Самодиагностирование электронного проекта модуля в целом (MED SD).

3. Построение модели отказов ИУС на основе СДПП

Согласно ISO/IEC 61508 [1] при построении модели отказов ИУС следует выделить множество безопасных (M_S) и множество M_D опасных отказов (отказов элементов/подсистем, влияющих на выполнение функций безопасности). Опасные отказы характеризуются интенсивностью λ_D. Для ИУС с СДПП множество опасных отказов разделяют на подмножества M_{DD} (detected dangerous failure, опасные отказы, выявленные СКД) и M_{DU} (undetected dangerous failure, опасные отказы, невыявленные СКД), которые характеризуются соответственно интенсивностями λ_{DD} и λ_{DU}.

Учитывая рассмотренные виды самодиагностирования, множество MDD формируется из шести подмножеств, как показано на рис. 3:

$$M_{DD}=\{M_{DD\ HWU},\ M_{DD\ HWM},\ M_{DD\ DTP},\ M_{DD\ RAD},\ M_{DD\ PD},\ M_{DD\ MED}\}.$$

Интенсивности отказов различных категорий определяются на основе процедур FMEDA (Failure Mode Effect and Diagnostic Analysis). После выделения подмножеств опасных детектируемых и опасных недетектируемых отказов компонент ИУС строится ее модель функционирования. Для ИУС с простой структурой интенсивности отказов системы в целом определяют как соответствующие суммар-

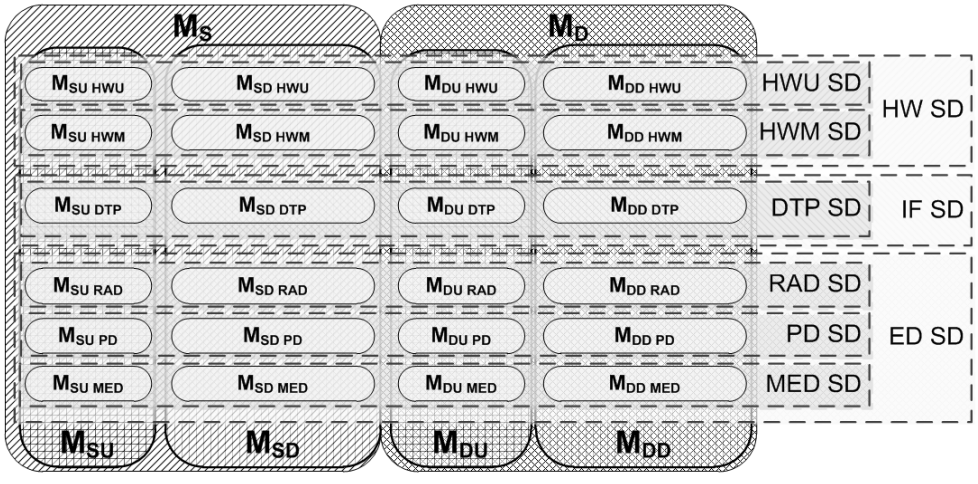

Рис. 3. Множества отказов ИУС на основе СДПП

ные интенсивности отказов $\sum\lambda_{DD}$ и $\sum\lambda_{DU}$.

Для случая, когда известны значения интенсивностей отказов и восстановлений системы в целом рассматривают марковскую модель отказов ИУС в общем виде. Такая модель представлена на рис. 4 и характеризуется следующими состояниями:

S_0 – начальное работоспособное состояние;

S_1 – отказ системы, выявленный СКД;

S_2 – отказ системы, невыявленный СКД;

S_3 – профилактическое техническое обслуживание (ПТО).

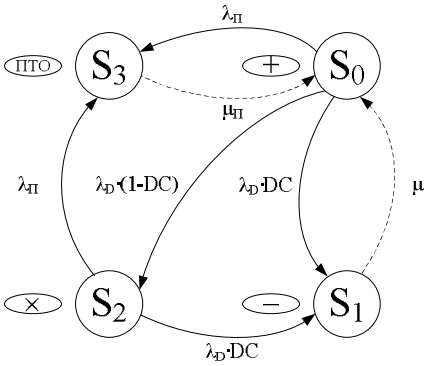

Рис. 4. Базовая марковская модель отказов ИУС

Часть опасных отказов, выявляемая автоматическими диагностическими тестами в неавтономном режиме определяется как диагностический охват (DC, diagnostic coverage) [9].

$$DC = \frac{\sum\lambda_{DD}}{\sum\lambda_{Dtotal}}, \qquad (2)$$

где $\sum\lambda_{DD}$ – суммарная интенсивность выявленных опасных отказов; $\sum\lambda_{Dtotal}$ – общая суммарная интенсивность опасных отказов.

Для модели на рис. 4 используются следующие допущения:

– опасные отказы распознаются с вероятностью выявления, равной DC;

– отказы, невыявленные СКД, возникают с вероятностью, равной дополнению величины диагностического охвата до единицы (1 – DC);

– после проявления отказов, невыявленных СКД, система в дальнейшем может перейти либо в состояние отказа, выявленного СКД, (после его проявления) либо в состояние ПТО;

– ПТО проводится с периодичностью $T_П=1/\lambda_П$ и с длительностью $T_{ПТО} = 1/\mu_П$.

В работах по теории надежности, например в [10], такие модели хорошо известны как модели систем со встроенным контролем и профилактикой. Однако применение таких моделей для оценки функциональной безопасности обязательно должно учитывать специфику предметной области, а именно: выделение подмножества опасных отказов, рассмотрение специфических (относительно теории надежности) режимов работы системы и результирующих показателей PFD – вероятности опасного отказа ФБ по запросу и PFH – средней вероятности опасных отказов ФБ в час.

4. Структурная схема надежности ИУС САЗ в режиме нормальной эксплуатации

Для сложных систем, к которым относятся ИУС САЗ, известны только параметры интенсивностей отказов и восстановлений компонент системы. Это обуславливает построение модели ИУС в виде структурной схемы надежности. Рассмотрим работу ИУС, которая является частью САЗ, в режиме нормальной эксплуатации (в установленных эксплуатационных пределах и условиях). САЗ включает три независимых аппаратных канала, каждый из которых диагностируется на наличие опасных отказов СКД. Структурная схема надежности ИУС, учитывающая мажоритарный контроль представлена на рис. 5.

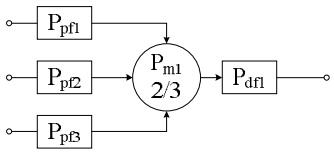

Рис. 5. Структурная схема надежности ИУС САЗ в режиме нормальной эксплуатации

Структурная схема надежности состоит из следующих компонент: P_{pf} – аппаратная составляющая каждого из трех каналов, описывает надежность аппаратной части системы (АС), P_{df} – программная составляющая (ПС), описывает надежность программной части системы (все каналы функционируют под управлением одинакового программного обеспечения) и P_m – определяет надежность мажоритарного элемента. Каждый из компонент (АС, ПС и мажоритарный элемент) характеризуется собственной моделью отказов. Так, модель отказов, описанная в предыдущем разделе, характерна для одного аппаратного канала. Модели отказов ПС и мажоритарного элемента проще и включают подмножества опасных и безопасных отказов.

Рассматриваемая система нормальной эксплуатации (СНЭ) функционирует в режиме с низкой частотой запросов к функциям безопасности. Соответственно, для оценки функциональной безопасности необходимо использовать показатель PFD_{avg} – средней вероятности опасного отказа ФБ по запросу. В

соответствии с [9], для моделей с ремонтом PFD_{avg} рассчитывается как сумма вероятностей нахождения в системе состоянии опасного отказа и ремонта.

На рис. 6 представлен вариант построения марковской модели функционирования ИУС в режиме СНЭ с учетом опасных отказов АС. При построении модели использованы следующие условные обозначения:

«+» – канал АС ИУС исправен;

«-» – в канале АС произошел отказ, детектируемый СКД;

«x» – в канале АС произошел недетектируемый СКД отказ;

«*» – мажоритарный элемент исправен;

«#» – мажоритарный элемент неисправен.

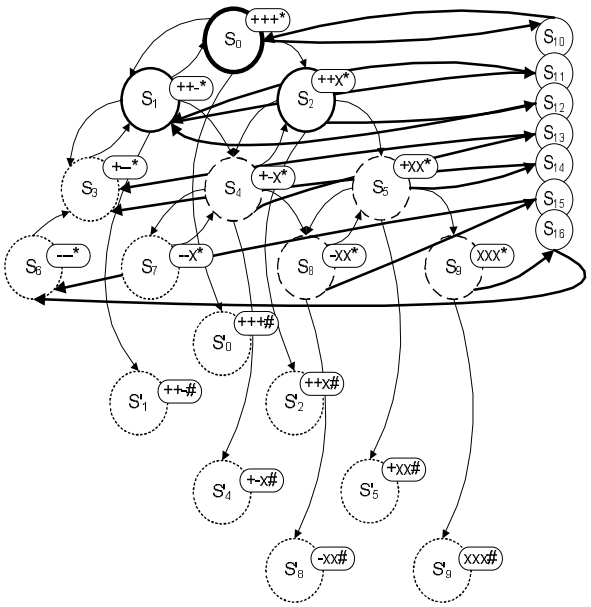

Рис.6. Марковская модель отказов и восстановлений АС ИУС в режиме СНЭ с профилактиками

Модель охватывает исправное состояние S_0, работоспособные состояния S_1 и S_2, в которых проявились соответственно по одному отказу из подмножеств M_{DD} и M_{DU} в аппаратных каналах, неработоспособные, но функционально безопасные состояния S_3, S_6, S_7, а также группа состояний {S'_0, S'_1, S'_2, S'_4, S'_5, S'_8, S'_9} (с отказом мажоритарного элемента). Состояния S_4, S_5, S_8, S_9 являются функционально небезопасными, так как в силу проявления нескольких недетектируемых опасных отказов мажоритарный элемент не в состоянии выявить отказ системы в целом. Состояния $S_{10}…S_{16}$ являются состояниями ПТО, при построении модели принято допущение, что ПТО позволяет выявить все проявившиеся недетектируемые отказы АС.

Расширения и модификации предложенной модели функционирования ИУС в режиме СНЭ будут рассмотрены в дальнейших исследованиях.

Заключение

Анализ построения ИУС систем аварийной защиты на основе СДПП показал, что:

а) алгоритмы самодиагностирования позволяют осуществлять три вида проверок – аппаратное самодиагностирование, программное самодиагностирование для интерфейсов передачи данных и программное самодиагностирование для электронного проекта ПЛИС;

б) проведение диагностических тестов осуществляется в режиме реального времени, что требует при построении марковских моделей ФБ использовать известные в теории надежности модели систем с встроенным контролем и диагностикой;

Приведен пример построения базовой марковской модели ИУС с учетом проявления отказов, выявленных и невыявленных СКД, при проведении диагностических тестов в режиме реального времени.

В то же время показано, что для структурной схемы надежности ИУС САЗ, функционирующей в режиме нормальной эксплуатации, необходимо построить марковскую модель, учитывающую, как минимум, подмножества опасных отказов трех аппаратных каналов (выявленных и невыявленных СКД) и мажоритарного элемента и программной версии системы. Построение и исследование таких моделей являются направлениями дальнейших исследований.

Литература

1. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements [Text]. – Impl. 01.05.2010. – Brussels: European Committee for Electrotechnical Standardization, 2010. – 68 p.

2. Системы управления и защиты ядерных реакторов [Текст] / под. ред. М. А. Ястребенецкого. – К. : Основа-Принт, 2011. – 768 с.

3. ГОСТ 26843-86. Реакторы ядерные энергетические. Общие требования к системе управления и защиты [Текст]. – введ. 01.03.1986. – М. : Стандартинформ, 1986. – 112 с.

4. Погосов, А. Ю. Технические средства управления ядерными реакторами с водой под давлением для АЭС [Текст] : учеб. / А. Ю. Погосов. – М. : Наука и техника, 2012. – 288 с.

5. Скляр, В. В. Анализ функциональной безопасности ИУС с использованием логических моделей ошибок контроля и управления [Текст] / В. В. Скляр // Радіоелектронні і комп'ютерні системи. – 2010. – №. 7(48). – С. 267-271.

6. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules [Text] / Y. Langeron, A. Barros, A. Grall, C. Berenguer // Journal of Loss Prevention in the Process Industries. – 2008. – № 21(4). – P.437-449.

7. Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС [Текст] / Е. С. Бахмач, А. А. Сиора, В. В. Скляр, В. И. Токарев, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 7(26). – С. 75-82.

8. Hashemian, H. M. Predictive maintenance in nuclear power plants through online monitoring [Text] / H. M. Hashemian // Nuclear and Radiation Safety Journal. – 2013. – № 4. – P. 42-50.

9. IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safetyrelated systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 [Text]. – Impl. 01.05.2010. – Brussels: European Committee for Electrotechnical Standardization, 2010. – 118 p.

10. Smith, W. E. Availability analysis of blade server systems [Text] / W. Earl Smith, Lorrie Tomek, Jerry Ackaret // IBM Systems Journal. – 2008. – Vol. 47, No. 4. – P. 621-640.

11. Ландрини, Г. Интегральные уровни безопасности в соответствии со стандартами МЭК 61508 и 61511 и анализ их связи с техническим обслуживанием [Текст] / Г. Ландрини // Стандартизация и сертификация. – 2009. – № 1. – С. 72-78.

Поступила в редакцию 30.10.2015, рассмотрена на редколлегии 18.11.2015

МОДЕЛІ ВІДМОВ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ НА ОСНОВІ САМОДІАГНОСТОВАНИХ ПРОГРАМОВАНИХ ПЛАТФОРМ В СИСТЕМАХ АВАРІЙНОГО ЗАХИСТУ РЕАКТОРІВ

В. В. Скляр, О. М. Одарущенко, Ю. Л. Поночовний, Є. М. Бульба, О. О. Івасюк

У статті розглянуто особливості побудови і функціонування системи аварійного захисту реакторів і її елемента - інформаційно-управляючої системи (ІУС) на основі самодіагностованої програмованої платформи. Виділено основні модулі ІУС, що дозволяють проводити діагностику і виявлення відмов в режимі реального часу. Наведено базову марковську модель функціонування ІУС, що враховує прояв виявлених і невиявлених відмов і проведення періодичних профілактик. Розглянуто структурну схему надійності ІУС в режимі нормальної експлуатації.

Ключові слова: інформаційно-управляюча система, функціональна безпека, система аварійного захисту реакторів, самодіагностована програмована платформа.

FAILURE MODES OF INFORMATION-CONTROL SYSTEMS BASED SELF-CHECKING SOFT PLATFORMS IN REACTOR PROTECTION SYSTEMS

V. V. Sklar, O. M. Odaruschenko, Y. L. Ponochovnyy, E. M. Bulba, O. O. Ivasjuk

The article describes the features of design and operation of the reactor protection system and its components - instrumentation and control system (ICS) based on programmable platform with self-diagnostic. The basic modules of ICS performs diagnostics and detection of failures in real time. Markov model is a basis for taking into account detected and undetected failures and periodical preventive maintenance. The reliability block diagram of ICS during normal operation is concidered.

Key words: instrumentation and control system, functional safety, reactor protection system, programmable platform with self-diagnostics.

Скляр Владимир Владимирович – д-р техн. наук, технический директор ПАО «Научно-производственное предприятие «Радий», Кировоград, Украина, e-mail: v.sklyar@radiy.com.

Одарущенко Олег Николаевич – канд. техн. наук, доцент, вед. науч. сотр., Научно-производственное предприятие «Радикс», Кировоград, Украина, e-mail: odarushchenko@gmail.com.

Поночовный Юрий Леонидович – канд. техн. наук, ст. науч. сотр., доцент кафедры компьютерной инженерии, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава, Украина, e-mail: pnch1@rambler.ru.

Бульба Евгений Николаевич – ст. науч. сотр., Научно-производственное предприятие «Радий», Кировоград, Украина, e-mail: e.bulba@radiy.com.

Ивасюк Александр Олегович – заместитель директора технического ПАО, «Научно-производственное предприятие «Радий», Кировоград, Украина. e-mail: ivasiuk.radiks@gmail.com.