УДК 629.039.58

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

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

ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ МОДУЛЕЙ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА ОСНОВЕ САМОДИАГНОСТИРУЕМЫХ ПРОГРАММИРУЕМЫХ ПЛАТФОРМ С ИСПОЛЬЗОВАНИЕМ ЗАСЕВА ДЕФЕКТОВ

В статье рассмотрены особенности обязательного этапа сертификационного тестирования системы аварийной защиты реакторов и ее ядра – информационно-управляющей системы (ИУС) на основе самодиагностируемой программируемой платформы методом засева дефектов. Выделены состояния и процедуры внесения критических и некритических дефектов в аппаратные модули. Приведена классификация модулей ИУС с позиции возможности репрезентативного засева дефектов. Показаны два case-study засева критического и некритического дефекта в модули ИУС. Рассмотрена диаграмма последовательности тестирования модулей ИУС, включающая засев дефектов.

Ключевые слова: *информационно-управляющая система, функциональная безопасность, засев дефектов, сертификация, тестирование.*

Введение

Для критических систем, таких как системы управления атомных электростанций (АЭС), выполнение сертификационных требований является актуальным и необходимым. Соблюдение всех требований, правил и норм позволяет избежать не только человеческих жертв, но и минимизировать риски любых ситуаций, которые могут к этому привести. 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. Базовый стандарт по функциональный безопасности ISO/IEC 61508 [1] рассматривает весь жизненный цикл электрических, электронных или программируемых электронных (E/E/PE) систем и изделий.

Согласно положений стандарта ISO/IEC 61508 сертификация подтверждает не только определенный уровень показателей функциональной безопасности, но и прохождение целого ряда обязательных процедур процесса жизненного цикла [2, 3]. При этом отдельные процедуры (в частности, тестирование) имеют расширенный состав стадий и фаз.

Постановка задачи исследования

Засев дефектов является важной и сложной частью анализа надежности и функциональной безопасности систем [4, 5]. 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 (САЗ) заключается в большом количестве и сложности модели резервирования элементов системы [6].

Цель данной статьи – освещение особенностей этапа сертификации платформы RadICS в части процесса тестирования с применением засева дефектов аппаратных модулей.

1. Состав и особенности реализации множества засеваемых дефектов

Согласно требований стандарта ISO/IEC 61508 [1] множество дефектов должно быть полностью реализовано на множестве элементов модуля. Конструктивные особенности FPGA (Field-Programmable Gate Array) схем не позволяют реализовать засев дефектов для всех элементов модуля (рис.1).

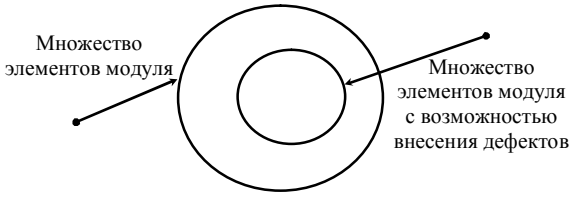


Рис.1. Множества элементов модуля и засеваемых дефектов

Процесс засева дефекта должен удовлетворять состояниям и переходам графов, представленных на рис. 2, где ключевыми моментами являются:

– засев дефекта не должен оказать влияние на алгоритмы функционирование модуля;

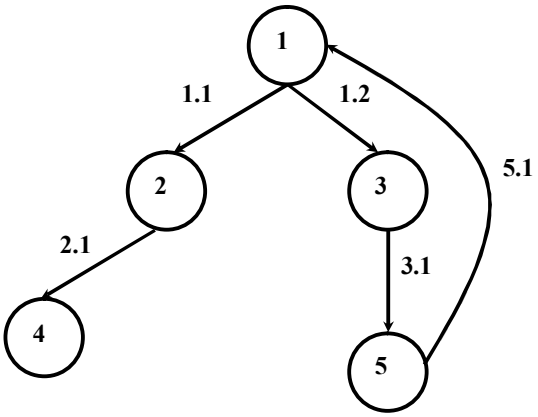
– после «высевания» (извлечения) дефекта из модуля он должен вернуться в рабочее состояние.

С точки зрения внесения дефекта все множество элементов модуля можно разделить на два основных подмножества рис. 3:

– набор элементов, размещение которых на поверхности модуля позволяет оказывать на них воздействие, назовем подмножеством «доступных» элементов;

– подмножеством «недоступных» элементов назовем набор элементов, монтаж которых не позволяет производить с ними манипуляции.

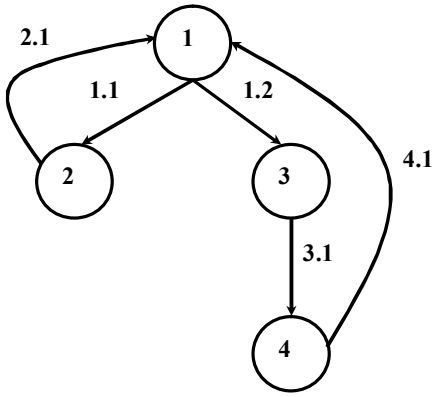
Из-за непригодности реализации тестирования путем «засева» дефектов подмножество «недоступных» элементов не рассматривается в данной работе.



а)

Состояния и процедуры-переходы:

- 1 – состояние модуля в исправном (рабочем) состоянии;
- 1.1. и 1.2 – дефект был внесен;
- 2 – самодиагностика не обнаружила внесенный дефект;
- 3 – самодиагностика обнаружила внесенный дефект;
- 2.1 – влияние дефекта, когда он не обнаружен самодиагностикой;
- 4 – неисправное состояние, при котором модуль не может выполнять свои функции;
- 3.1 – действие платформенной логики при обнаруженном дефекте;
- 5 – безопасное состояние модуля;
- 5.1 – «высевание» дефекта из модуля



б)

Состояния и процедуры-переходы:

- 1 – состояние модуля в исправном (рабочем) состоянии;
- 1.1. и 1.2 – дефект был внесен;
- 2 – самодиагностика модуля не обнаружила внесенный дефект;
- 3 – самодиагностика модуля обнаружила внесенный дефект;
- 2.1 – удаление дефекта из модуля;
- 3.1 – действие логики приложения при обнаруженном дефекте;
- 4 – состояние модуля, определенное логикой приложения;
- 4.1 – «высевание» дефекта из модуля

Рис. 2. Графы состояний модуля при внесении критического (а) и некритического (б) дефектов

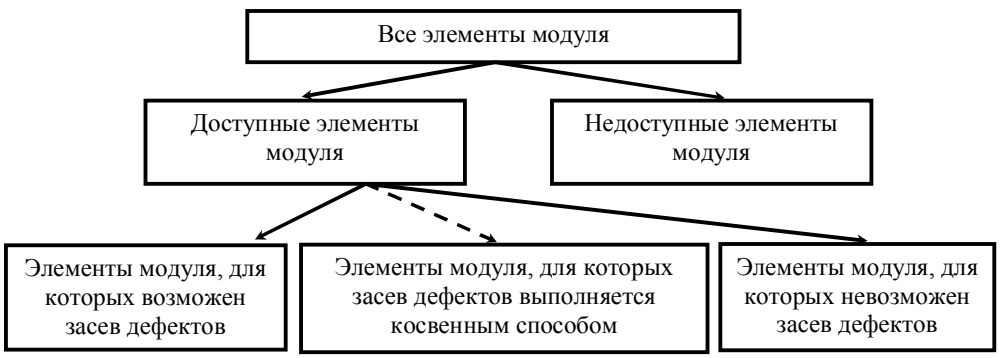


Рис. 3. Классификация элементов модуля с точки зрения внесения дефектов

Подмножество «доступных» элементов в свою очередь можно разделить на следующие группы:

– группа элементов, воздействия на которые приведет к «прямому» засеву одно из множества необходимых дефектов;

– группа элементов, влиянием на которые невозможно внести дефект в модуль;

– группу элементов, при воздействии на которые, возможно создать в модуле последствия внесения одного из необходимых дефектов назовем группой «косвенных» элементов.

В приведенной на рис. 3 классификации наибольший интерес представляет группа элементов, через которые возможно сгенерировать последствия от «засева» дефекта, который невозможно внести напрямую.

2. Case-study засева дефектов в модули ИУС САЗ

Каждый раз, когда возникает коллизия между необходимостью выполнения «засева» дефекта и нарушением основных правил такого выполнения, необходимо рассмотреть возможность «засева» дефекта, через использование элементов «косвенной» группы. Рассмотрим более детально случаи применения элементов модуля, относящихся к группе «косвенных» элементов. Предположим, что необходимо проверить реакцию модуля на изменение одного из его внутренних напряжений на ±10% от номинального значения – VDC_{nom}. Существуют два пути засева такого дефекта. Первый путь – это влияние на элементы, непосредственно участвующие в формировании такого напряжения, т.е. элементы «прямой» группы. Но это невозможно, если такая реализация «дефекта» приведет к тому, что после его высевания модуль не вернется в рабочее и исправное состояние. Второй путь – реализация дефекта через подключение в разрыв цепи прецизионного внешнего источника питания. И далее его помощью осуществление девиации напряжения от его номинального значения в указанных пределах. Но такой подход приведет к изменению алгоритмов функционирования модуля. Так как, модуль не перейдет в безопасное состояние – обесточивание всех узлов. Вследствие того, что внешний источник питания будет продолжать питать определенные узлы модуля.

Анализ рассматриваемого дефекта позволяет сделать вывод о том, что главным последствием его засевания является изменение значения напряжения на входе аналого-цифрового преобразователя (АЦП), которое стоит перед входом устройства, выполняющего функции контроля напряжения (WatchDog). Изменяя, напряжение на входе АЦП имитируется возникновение данного дефекта в модуле, не нарушая алгоритмов функционирования модуля, проверяется его реакция на внесенный дефект и после высевания дефекта модуль вернется в исправное (рабочее) состояние.

С помощью такого подхода было реализовано «засевание» дефекта 5VDC±10% в узел PSWD модулей I/O (рис. 4) во время интеграционного тестирование в рамках сертификации модулей, произведенных научно-производственным предприятием «Радий» по уровню SIL3 в соответствие со стандартом IEC 61508 [1].

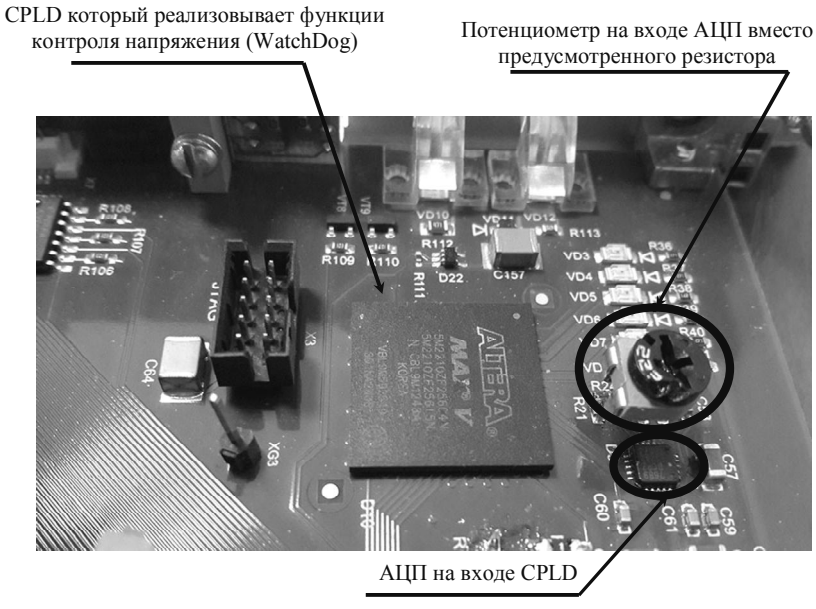


Рис. 4. Иллюстрация «засева» критического дефекта в узел PSWD через элементы «косвенной» группы

На рис. 5 изображен не критический дефект – изменение напряжения питающего операционный усилитель в узле Analog Input Unit (AIU) в тракте обработке сигнала, принятого от полевой цепи, внесенный в Analog Input Module (AIM). Из-за невозможности внести данный дефект через группу «прямых» элементов, были проанализированы последствия от наличия такого дефекта.

Если бы такая девиация имела место, то микросхема, отвечающая за контроль данного напряжения, сгенерировала бы соответствующий сигнал в FPGA. Поэтому, было принято решение изменить напряжение на входе данной микросхемы (рис. 5).

3. Этапы тестирования с выполнением засева дефектов

На основе вышеизложенного материала и информации, представленной в работах [2, 4, 7], весь процесс подготовки и выполнения тестирования методом «засева» дефектов может быть представлен следующей диаграммой последовательности (рис. 6).

Особое внимание во время тестирования следует обратить на формирование «ожидаемого» результата, который и будет той разницей в состояниях модуля до и после внесения дефекта. Так, для критических дефектов, «ожидаемым» результатом будет переход модуля в состояние «FAULTED MODE» с обесточиванием всех узлов модуля. Для не критических дефектов «ожидаемым» результатом является индикация о наличии ошибки на средствах отображения модуля, а дальнейшие действия будут определяться реализованной логикой приложения.

Заключение

В статье был рассмотрен путь реализации тестирования методом «засева» дефектов, через группу элементов, которые не связаны напрямую с вносимым дефектом. Рассмотрены диаграммы состояний и переходов, моделирующие внесение критических и некритических дефектов в аппаратные каналы модулей ИУС САЗ. Так же, в статье была предложена новая классификация элементов модуля с точки зрения внесения дефектов. На практических примерах показан засев аппаратных дефектов в модули ИУС САЗ.

Особое внимание было уделено методике засева дефектов через элементы «косвенной» группы, так как она позволяет реализовать условие возврата модуля в рабочее состояние после высевания дефекта. В Case-study продемонстрированы засевы критического и некритического аппаратных дефектов.

На основе предложенного и существующих [4, 5] методов реализации засева дефектов была разработана диаграмма последовательности процедуры выполнения засева аппаратных дефектов (Hardware FIT - Fault-Injection Testing).

Дальнейшими путями развития являются:

– рассмотрение особенностей внесения дефекта в модули приема и обработки информации датчиков нейтронного потока;

– реализация засева дефектов в память FPGA;

– требования к разработке и применению специализированных программно-аппаратных средств для выполнения засева дефектов.

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. Скляр, В. В. Сертификация информационно-управляющей платформы на базе ПЛИС на соответствие требованиям по функциональной безопасности стандарта МЭК 61508 [Текст]/ В. В. Скляр // Ядерна та радіаційна безпека. – 2013. – Вип. 4. – С. 54-60.

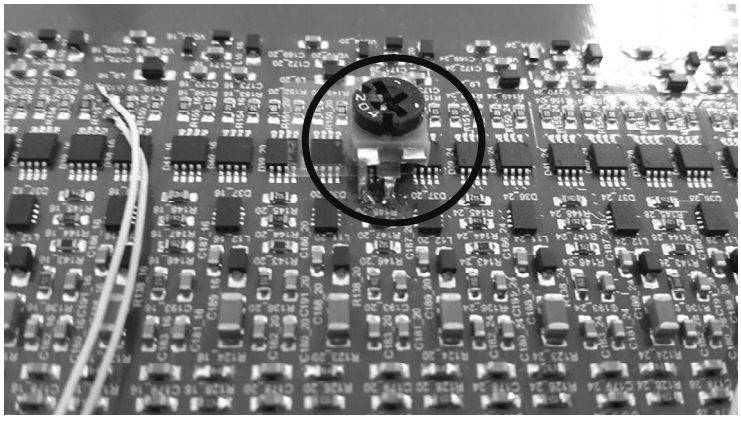


Рис. 5. Иллюстрация «засева» некритического дефекта в узел AIU модуля AIM через элементы «косвенной» группы

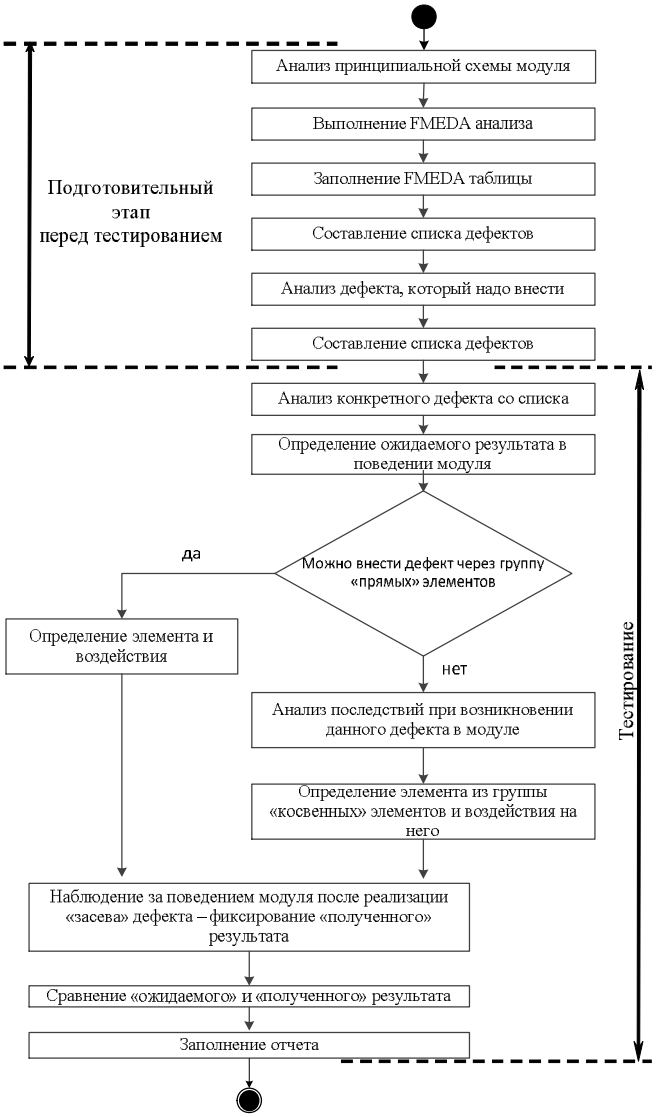


Рис. 6. Диаграмма последовательности выполнения тестирования с выполнением засева дефектов и процедур FMEDA (Failure Modes Effects and Diagnostic Analysis)

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

4. Kharchenko, V. Multy-fault injection testing: cases for FPGA-based NPP I&C systems [Text] / V. Kharchenko, O. Odarushchenko, V. Sklyar // Proceedings of ICONE-23 23rd International Conference on Nuclear Engineering, May 17-21, 2015, Chiba, Japan. – P. 8.

5. Kharchenko, V. Fault-injection testing: FIT-ability, optimal procedure and tool for FPGA-based systems SIL certification [Text] / V. Kharchenko, V. Sklyar, O. Odarushchenko, A. Ivasuyk, // Proceedings of Design & Test Symposium, 2013 East-West, Rostov-on-Don, 2013. – P. 1-5.

6. 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.

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.

References

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

2. Sklyar V. V. Sertifikatsiya informatsionno-upravlyayushchei platformy na baze PLIS na soot-vetstvie trebovaniyam po funktsional'noi bezopas-nosti standarta MEK 61508 [Certification of a information control platform on the FPGA base on compliance to requirements for the functional safety of the IEC61508]. *Nuclear that radiation safety*, 2013, no. 4, pp. 54-60.

3. *Sistemy upravleniya i zashchity yadernykh reaktorov* [Control and protection systems of nuclear reactors]. M. A. Yastrebenetskii (edits). Kiev, Osnova-Print Publ., 2011. 768 p.

4. Kharchenko, V. S., Odarushchenko, O. M., Sklyar, V. V. Multy-fault injection testing: cases for FPGA-based NPP I&C systems. *Proceedings of ICONE-23 23rd International Conference on Nuclear Engineering*, 2015, pp. 8.

5. Kharchenko, V. S., Odarushchenko, O. M., Sklyar, V. V. Ivasuyk, A. O. Fault-injection testing: FIT-ability, optimal procedure and tool for FPGA-based systems SIL certification. *Proceedings of Design & Test Symposium*, 2013, pp. 1-5.

6. Sklyar, V. V. Analiz funktsional'noi bezopasnosti IUS s ispol'zovaniem logicheskikh modelei oshibok kontrolya i upravleniya [The analysis of the functional safety of ICS with use of logical models of monitoring and control errors]. *Radioelectronic and computer systems*, vol.7, no. 48, 2010, pp. 267-271.

7. Bakhmach, E. S. Siora, A. A., Sklyar, V. V., Tokarev, V. I., Kharchenko, V. S. Obespechenie i otsenka bezopasnosti informatsionnykh i upravlyayushchikh sistem AES na baze PLIS [Providing and assessment of safety of the informational and control NPPs systems on the FPGA base] *Radioelectronic and computer systems*, vol.7, no. 26, 2007, pp. 75-82.

Поступила в редакцию 5.04.2016, рассмотрена на редколлегии 14.04.2016

ПРОЦЕДУРИ ТЕСТУВАННЯ МОДУЛІВ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ НА ОСНОВІ САМОДІАГНОСТОВАНИХ ПРОГРАМОВАНИХ ПЛАТФОРМ З ВИКОРИСТАННЯМ ЗАСІВУ ДЕФЕКТІВ

О. О. Івасюк, Ю. Л. Поночовний, Є. М. Бульба

У статті розглянуті особливості обов'язкового етапу сертифікаційного тестування системи аварійного захисту реакторів і її ядра - інформаційно-управляючої системи (ІУС) на основі самодіагностованої програмованої платформи методом засіву дефектів. Виділено стани і процедури внесення критичних і некритичних дефектів в апаратні модулі. Наведено класифікацію модулів ІУС з позиції можливості репрезентативного засіву дефектів. Показані два case-study засіву критичного і некритичного дефекту в модулі ІУС. Розглянуто діаграму послідовності тестування модулів ІУС, що включає засів дефектів.

Ключові слова: інформаційно-управляюча система, функціональна безпека, засів дефектів, сертифікація, тестування.

THE FAULT-INJECTION TESTING OF INSTRUMENTATION AND CONTROL SYSTEM MODULES BASED ON SELF-DIAGNOSTIC PROGRAMMABLE PLATFORMS

A. O. Ivasjuk, Y. L. Ponochovnyi, E. M. Bulba

In the article were described the special aspects as a required step for certification testing of the reactor protection systems and its core - instrumentation and control system (ICS) based on the self-diagnosable and programmable platform by using method of fault-injection. In the article were outlined states and procedures of fault-injection for critical and non-critical faults in the module's hardware. The classification of ICS modules was referred from a perspective of possibility representative fault-injection. The two case-study injections were showed for critical and non-critical faults in the ICS modules. Was considered the diagram of sequence of testing of ICS modules including fault-injection.

Key words: instrumentation and control system, functional safety, fault-injection, certification, testing.

Ивасюк Александр Олегович – канд. техн. наук, заместитель директора технического научно-производственного предприятия «Радий», Кировоград, Украина. e-mail: ivasiuk.radiks@gmail.com.

Поночовный Юрий Леонидович – канд. техн. наук, ст. науч. сотр., доцент кафедры компьютерной инженерии Полтавского национального технического университета им. Юрия Кондратюка, Полтава, Украина. e-mail: pnch1@rambler.ru.

Бульба Евгений Николаевич – ст. науч. сотр. научно-производственного предприятия «Радий», Кировоград, Украина, e-mail: e.bulba@radiy.com.

Ivasjuk Aleksandr Olegovich - PhD, Deputy Head of Technical director "Radiy", Kirovograd, Ukraine. e-mail: ivasiuk.radiks@gmail.com.

Ponochovnyi Yurii Leonidovich - PhD, Senior Researcher, Associate Professor of Computer Engineering, Poltava National Technical University, Poltava, Ukraine. e-mail: pnch1@rambler.ru.

Bulba Evgenyi Nikolaevich - Senior researcher "Radiy", Kirovograd, Ukraine. e-mail: e.bulba@radiy.com.