РАДИОТЕХНИКА И ЭЛЕКТРОНИКА, 2022, том 67, № 5, с. 514–519

ФИЗИЧЕСКИЕ ПРОЦЕССЫ В ЭЛЕКТРОННЫХ ПРИБОРАХ

УДК 621.382

ДИАГНОСТИКА СОСТОЯНИЯ БЛОКОВ МИКРОКОНТРОЛЛЕРА С ПОМОЩЬЮ ВСТРОЕННЫХ СРЕДСТВ ОТЛАДКИ ПРИ ВОЗДЕЙСТВИИ НЕЙТРОННОГО И ТОРМОЗНОГО ИЗЛУЧЕНИЙ

© 2022 г. А. С. Пилипенко*

Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт технической физики им. акад. Е.И. Забабахина, ул. Васильева, 13, Снежинск, 456770 Российская Федерация

**E-mail: pilipenko_anatol@mail.ru*

Поступила в редакцию 12.06.2021 г.
После доработки 06.09.2021 г.
Принята к публикации 10.09.2021 г.

Для сложно-функционального устройства типа микроконтроллера (МК) исследована возможность использования встроенных средств отладки для контроля внутренних блоков при воздействии ионизирующего излучения. Оценены значения сечений одиночных сбоев в различных блоках МК, возникающих при облучении нейтронами с энергией 14 МэВ. Определены характерные области нарушения функционирования МК при воздействии импульса тормозного излучения.

DOI: 10.31857/S0033849422050096

ВВЕДЕНИЕ

Современные микроконтроллеры (МК) содержат в своем составе помимо вычислительного ядра большое число различных по назначению периферийных блоков (порты ввода-вывода, интерфейсы, таймеры и др.). Задача контроля состояния такого функционально сложного объекта при воздействии ионизирующих излучений (ИИ) в общем случае заключается в том, чтобы зафиксировать факт сбоя, определить причину его возникновения и блок МК, в котором он произошел [1]. Задача является методически и экспериментально сложной, поскольку необходимо решить целый ряд вопросов: определить состав и режим работы контролируемых блоков, организовать доступ и обмен информацией с ними в условиях удаленности объекта исследований и контрольного оборудования и т.д. Сюда же следует отнести учет особенностей конкретного источника ИИ и/или вида воздействия. К примеру, вследствие высокой проникающей способности нейтронов расположение промежуточных блоков управления и согласования вблизи объекта исследований если и является принципиально возможным, то требует применения мер снижения воздействия на такие блоки (например, экранирования).

В настоящее время контроль встроенных блоков при воздействии ИИ обычно выполняется с помощью микропрограммы, исполняемой самим объектом исследования (т.е. МК) [2]. При этом диагностическая информация (в виде результатов выполнения вычислительных операций, содержимого внутренних блоков данных и т.п.) передается внешнему контрольному оборудованию непосредственно через какой-либо интерфейс, который входит в состав МК [3].

Другим способом для контроля сбоев при выполнении программы является использование встроенных средств отладки, которые поддерживаются большинством современных МК. Так, например, авторы [4] используют блок трассировки МК с ядром ARM для анализа сбоев, возникающих при статическом облучении нейтронами атмосферного спектра. МК был реализован на базе системы-на-кристалле, анализ диагностической информации осуществляется блоком в составе системы и вывод информации производится через последовательный интерфейс в составе МК.

Описанные способы не лишены недостатков. Получение диагностической информации от МК становится невозможным в случае его зависания, что часто происходит при воздействии импульсного ИИ [5]. Кроме того, объем такой информации сильно зависит от функционала исполняемой программы.

Выбор встроенных средств отладки для контроля состояния внутренних блоков МК в данной работе обусловлен несколькими причинами.

Во-первых, подобные средства МК с ядром ARM посредством прямой адресации предоставляют доступ к адресному пространству МК (в которое отображаются все регистры встроенных периферийных блоков). Дополнительно из области

управления системой посредством косвенной адресации доступны регистры ядра, такие как регистры общего назначения (РОН), регистр флагов, регистр стека и др. Другими словами, через встроенные средства отладки возможно контролировать состояние всех внутренних регистров МК. Данный способ контроля внутренних регистров МК не зависит от функционала исполняемой МК программы и в предельном случае может осуществляться даже при ее отсутствии.

Во-вторых, доступ к встроенным средствам отладки может осуществляться несколькими способами, например, с помощью методологии граничного сканирования. При такой организации доступа может возникнуть вопрос о возможных сбоях в работе средств отладки при воздействии ИИ. Предварительный анализ показывает, что:

а) регистры контроллера интерфейса обмена данными и системы отладки содержат точно такие же запоминающие ячейки, как и, к примеру, оперативное запоминающее устройство (ОЗУ). При воздействии нейтронов в них, вообще говоря, могут возникать обратимые локальные эффекты типа одиночных сбоев (ОС) – инвертирование ячеек памяти. Однако общее число чувствительных к эффекту ячеек в этих регистрах много меньше суммарного числа ячеек в ОЗУ и регистрах периферийных блоков, следовательно, вероятностью появления ОС в них можно пренебречь (так как эта вероятность пропорциональна объему рассматриваемой памяти). К тому же регистры средств отладки сами не хранят данные, а работают в режиме “запрос-выборка из памяти МК-передача контроллеру”, поэтому в случае сбора данных после воздействия или в паузе между периодами облучения эффект ОС вообще не влияет результат эксперимента;

б) при воздействии импульса ИИ считывание информации, т.е. основная работа средств отладки, происходит после воздействия, в установившемся режиме. Поэтому непосредственно на процесс сбора данных импульс ИИ не может оказывать влияния. В сам момент воздействия контроллер интерфейса обмена данными находится в режиме ожидания и возникающая при протекании радиационно-наведенного тока импульсная помеха не должна приводить к нарушениям в его функционировании. Кроме того, в средствах отладки предусмотрена функция отключения питания основных схем поддержки отладки, которую можно использовать на время действия импульса ИИ, что еще больше снизит вероятность сбоя в работе.

Таким образом, цель данной работы – определить возможности встроенных средств отладки МК с ядром ARM по контролю состояния внутренних блоков МК при воздействии нейтронного и тормозного излучений.

1. МЕТОДИКА ИЗМЕРЕНИЙ

В качестве объекта исследования был использован МК с ядром ARMv7, изготовленный по технологии “объемный кремний” с топологической нормой 0.18 мкм. Для организации обмена данными со встроенными средствами отладки МК использовались аппаратный контроллер интерфейса отладки (ИО) на базе микросхемы FT2232H и программное обеспечение собственной разработки, предоставляющее наиболее полный и гибкий доступ к компонентам отладочного интерфейса МК.

Контроль состояния внутренних блоков МК осуществляли при облучении нейтронами с энергией 14 МэВ и при воздействии импульса тормозного излучения. В зависимости от вида ИИ ставились разные цели экспериментов.

При облучении нейтронами с энергией 14 МэВ целью была демонстрация возможности прямой экспериментальной оценки чувствительности управляющих регистров и массивов памяти различных функциональных блоков МК к ОС. Особенностью постановки эксперимента является то, что в данном случае в памяти программ МК отсутствовала исполняемая программа и МК находился в режиме ожидания. Это позволило проводить оценку именно одиночных, а не функциональных сбоев, которые имели бы место в случае работы МК на штатной частоте в процессе облучения. Эксперимент проводили при облучении в статическом режиме с плотностью потока нейтронов порядка 10^9 н/(см^2 с) с периодическим чтением данных из управляющих регистров и массивов памяти функциональных блоков МК. Чтение информации происходило с накоплением, т.е. после чтения информация не перезаписывалась. Подсчет числа ОС осуществлялся путем сравнения информации до и после облучения. Обобщенная структурная схема эксперимента приведена на рис. 1. Для подключения МК использовались четыре сигнальные линии ИО и одна линия питания (общая для МК и буферного повторителя). Измерение флюенса нейтронов осуществляли с помощью активационной методики (погрешность $\pm 20\%$).

При воздействии импульса тормозного излучения целью была проверка возможности контроля состояния внутренних блоков МК в случае его зависания и, в случае успешности контроля, определение причин такой реакции по анализу полученной диагностической информации. В данном случае МК работал в режиме исполнения программы из внутренней памяти программ с подключенным ИО. Функционал программы заключался в формировании периодического сигнала (меандра) с частотой 0.5 МГц на одном из выводов МК. Источник тактирования МК – встроенный RC-генератор на частоте 8 МГц, частота работы ядра 80 МГц. Используемые функ-

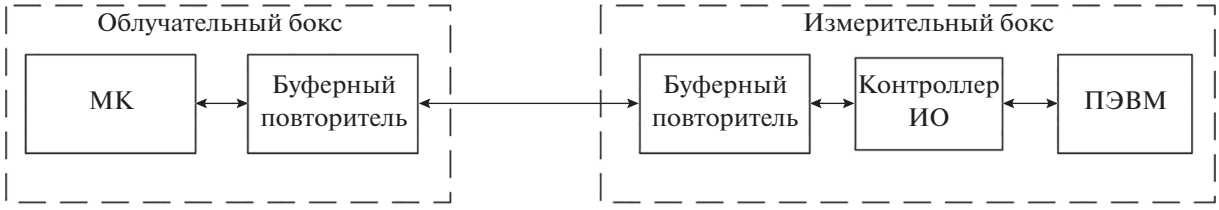

Рис. 1. Структурная схема эксперимента.

циональные блоки: блок умножителя частоты PLL, порт ввода-вывода PORTA, блок управления тактовыми частотами, таймер общего назначения. Для определения факта сбоя (зависания) МК в момент воздействия импульса тормозного излучения с помощью осциллографа контролировался меандр, генерируемый МК. Под сбоем в данных экспериментах понимается кратковременное прекращение генерации меандра, под зависанием – прекращение генерации до момента переинициализации МК (переключение питания). Структурная схема эксперимента в целом повторяет приведенную на рис. 1. Отличием является использование независимых линий питания МК и буферного повторителя, а также наличие выделенной сигнальной линии для контроля меандра. Обобщенная схема включения МК приведена на рис. 2.

В качестве параметра, характеризующего отклик объекта на импульс тормозного излучения, часто используется ток потребления. Для его контроля проводили отдельные эксперименты, в которых представленная на рис. 2 схема дополнялась токоизмерительным резистором в цепи питания номиналом ~1 Ом. Напряжение на этом резисторе контролировали с помощью осциллографа.

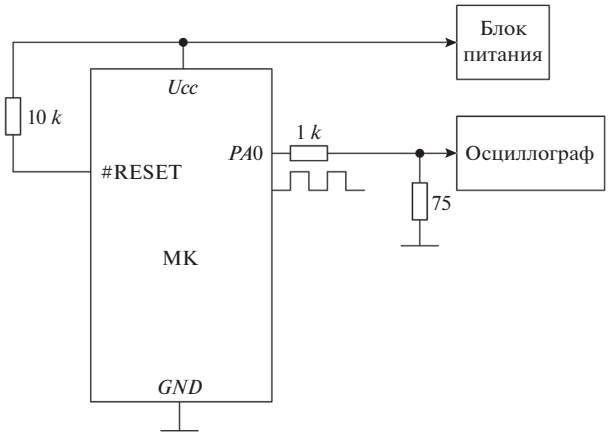

Рис. 2. Обобщенная схема включения МК (линии связи с ИО и буферные повторители не показаны).

В экспериментах также контролировался факт наличия/отсутствия доступа к ИО после воздействия. Измерение экспозиционной дозы в импульсе осуществляли с помощью термолюминисцентной методики (погрешность ±20%).

2. РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТОВ

На рис. 3 представлены зависимости числа ОС (N) от флюенса нейтронов F с энергией 14 МэВ, полученные при облучении МК. Данные по числу ОС представлены отдельно для встроенного ОЗУ МК (линия *1*) и для периферии (линия *2*). В периферию здесь включены РОН и другие регистры ядра, регистры блока управления тактовыми сигналами, портами ввода-вывода, таймерами, интерфейсами приема-передачи и др. (в общей сложности регистры порядка 30 блоков). Во всех исследованных блоках наблюдаются ОС, однако ввиду статистически малозначимого числа ОС в

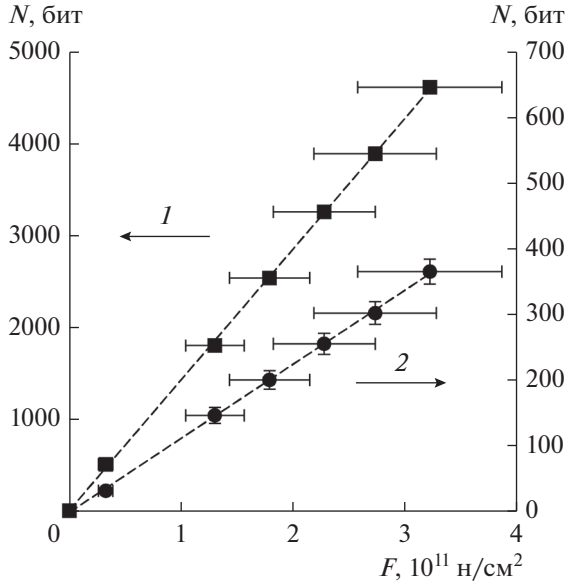

Рис. 3. Зависимости числа ОС (N) от флюенса нейтронов F в блоках МК: квадраты – ОЗУ (*1*); кружочки – периферийные блоки (*2*); штриховые линии – линейная аппроксимация.

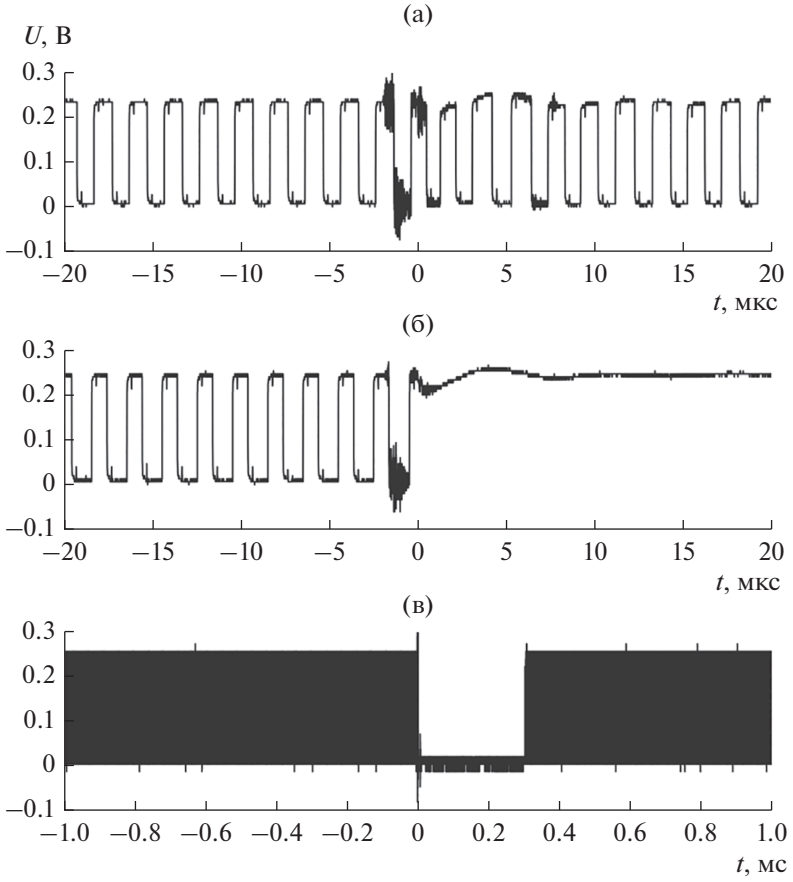

Рис. 4. Осциллограммы с выхода МК при различных значениях мощности экспозиционной дозы: 1.2×10^9 (а), 2×10^9 (б) и 3×10^9 Р/с (в).

отдельных блоках на рис. 3 приведено общее число ОС во всех блоках.

Как видно из рис. 3, зависимости $N(F)$ имеют характерный вид – прямая, пересекающая начало координат. Такой вид зависимостей позволяет оценить основную характеристику чувствительности МК к эффекту ОС – сечение σ, которое является отношением общего числа ОС к флюенсу частиц: $\sigma = N/F$. Определяемое по данному выражению значение сечения ОС составляет $(1.4 \pm \pm 0.3) \times 10^{-8}$ см^2 для ОЗУ и $(1.0 \pm 0.2) \times 10^{-9}$ см^2 для периферийных блоков.

В экспериментах по исследованию воздействия импульса тормозного излучения на МК наблюдается четыре типа реакции, каждая в своем диапазоне уровней воздействия. Типы описаны ниже в порядке их проявления при возрастании уровня нагружения.

Реакция типа 1. Отсутствие сбоев в функционировании либо кратковременное изменение (порядка 10^{-5} с) частоты/амплитуды меандра без срыва генерации.

Реакция типа 2. Зависание (прекращение генерации тестового сигнала), при этом доступен ИО, позволяющий получить информацию о состоянии функциональных блоков МК.

Реакция типа 3. Кратковременный сбой в функционировании (срыв генерации меандра) длительностью порядка 300 мкс с последующим восстановлением работоспособности, ИО доступен.

Реакция типа 4. Зависание, ИО недоступен.

Получены типовые осциллограммы контролируемого сигнала (рис. 4), иллюстрирующие наблюдаемые типы реакций (импульс воздействия длительностью 30 нс в момент времени $t = 0$).

Определена зависимость амплитуды ионизационного тока МК от мощности экспозиционной дозы (рис. 5). Видно, что зависимость имеет тенденцию к насыщению при мощности дозы порядка 5×10^9 Р/с.

3. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Сечения ОС, оцененные по результатам экспериментов при облучении МК нейтронами, для ОЗУ и периферии отличаются примерно на порядок. Однако чувствительность к ОС напрямую за-

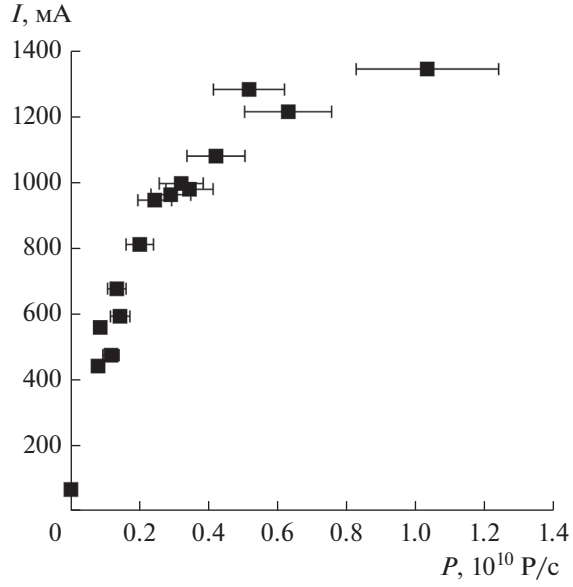

Рис. 5. Зависимость амплитуды ионизационного тока I от мощности экспозиционной дозы P.

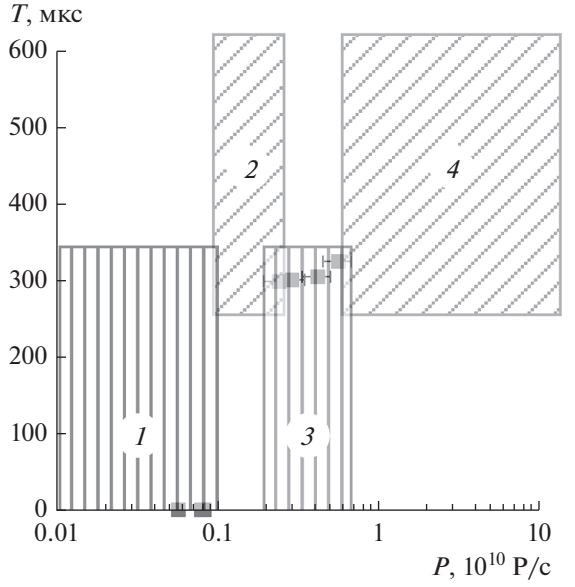

Рис. 6. Зависимость ВПР T от экспозиционной дозы P; *1–4* – области разных типов реакции МК.

висит от числа рассматриваемых элементов (ячеек памяти), в которых может возникнуть эффект. Поэтому на практике для сравнения чувствительностей различных объектов используют приведенную величину – сечение на 1 бит. В результате пересчета получаются значения $(5.4 \pm 1.1) \times 10^{-14}$ см^2/бит для ОЗУ и $(5.3 \pm 1.1) \times 10^{-14}$ см^2/бит для периферийных блоков.

По результатам можно сделать следующие выводы об объекте исследований:

1) линейный вид зависимости $N(F)$ для ОЗУ на рис. 3 указывает на то, что ОЗУ не защищено от ОС помехоустойчивым (избыточным) кодированием, поскольку в таком случае зависимость $N(F)$ была бы нелинейной на начальном участке [6];

2) близкие значения сечений/бит ОС для ОЗУ и периферии позволяют предположить, что запоминающие ячейки ОЗУ и управляющих регистров периферийных блоков, включая регистры ядра процессора, схемотехнически одинаковы. То есть их чувствительность к эффекту ОС определяется главным образом топологическими нормами, по которым изготовлен МК.

Данные выводы получены только из экспериментальных данных, однако довольно точно характеризуют исследуемый МК, в котором действительно не применяется никаких специальных мер для повышения стойкости к ИИ. Это свидетельствует о возможности применения рассматриваемого метода контроля состояния внутренних блоков МК при облучении нейтронами.

На рис. 6 представлены зависимости времени потери работоспособности (ВПР) МК от мощности экспозиционной дозы P, где ВПР оценивалось по осциллограммам выходного меандра, генерируемого МК. Цифрами обозначены области разных типов реакции МК (типы реакций описаны выше).

Использование ИО МК позволяет получить информацию о состоянии внутренних блоков, которая может быть использована для поиска причин сбоев в работе (области 2 и 3 на рис. 6).

В области 2 МК зависает и получение информации о его состоянии возможно только через ИО. Анализ содержимого регистров процессорного ядра, ОЗУ (как хранилища стека) и блока управления системой указывает на то, что контроллер пытается выполнить недопустимую инструкцию. Это приводит к вызову обработчика исключения типа тяжелого отказа, из которого контроллер выйти не может. При этом примерно в половине случаев в стек успевает записаться содержимое регистров процессора, необходимых для корректного выхода из обработчика исключения. Такая реакция МК может быть обусловлена либо возникновением радиационно-наведенной импульсной помехи на внутренних токопроводящих дорожках ИС, либо превышением максимально допустимой скорости изменения напряжения питания (что приводит к сбоям тактирования).

В области 3 генерация меандра восстанавливается примерно через 300 мкс после воздействия. Поскольку в момент воздействия возникает просадка напряжения питания (это подтверждается насыщением зависимости тока от мощности экспозиционной дозы [7], рис. 5), то такая реакция могла бы означать активацию внутреннего сигна-

ла сброса Power-On-Reset при снижении напряжения питания ниже минимально допустимого. Однако в этом случае время восстановления функционирования для данного МК составляло бы порядка 4 мс. Для определения факта возможного перезапуска МК в некоторых неиспользуемых в основной программе регистрах с помощью ИО устанавливались биты-маркеры. В случае сброса при последующем чтении эти биты были бы сброшены в начальное состояние. Как показали эксперименты, МК действительно входит в состояние сброса. По-видимому, такая реакция вызвана формированием импульса сброса на выводе RESET, который подтянут к питанию через резистор сопротивлением 10 кОм.

ЗАКЛЮЧЕНИЕ

Таким образом, отработан метод контроля состояния внутренних блоков МК с ядром ARM с помощью встроенных средств отладки, который позволяет считывать информацию из регистров различных блоков памяти и периферии и проводить анализ изменения информации.

В экспериментах по облучению исследуемого МК нейтронами с энергией 14 МэВ оценены чувствительности различных блоков МК к эффекту ОС. Совпадающая в пределах погрешности чувствительность ОЗУ и регистров периферийных блоков подтверждает предположение об одинаковой схемотехнической организации запоминающих ячеек отдельных блоков. Продемонстрирована возможность применения метода для МК, работающего без исполняемой программы, что позволяет исключить влияние на результаты экспериментов функционала исполняемой программы.

При воздействии импульса тормозного излучения в зависимости от уровня воздействия наблюдается несколько типов реакции МК: временные сбои функционирования и зависания. Применение средств отладки позволяет в ряде случае получить дополнительную информацию для объяснения такого поведения МК, что зачастую невозможно при использовании методов контроля, в которых сам МК является источником диагностической информации о состоянии встроенных блоков.

В качестве преимущества предлагаемого метода следует указать высокую степень его унификации. Это обусловлено тем, что структура и алгоритмы доступа к встроенным средства отладки определяются только спецификацией на процессорное ядро ARM. Поэтому при смене исследуемого объекта могут потребоваться минимальные изменения аппаратной (переназначение контактов разъема) и программной части (переназначение базовых адресов и размеров периферийных блоков).

Автор заявляет об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. *Некрасов П.В.* Методы и средства прогнозирования радиационной стойкости микропроцессорных СБИС. Дис. ... канд. техн. наук. Москва: Национальный исследовательский ядерный университет МИФИ, 2010. 120 с.
2. *Кравченко Н.Д., Лоскутов И.О., Некрасов П.В. и др.* // Тр. 23-й Всерос. научн.-техн. конф. “Стойкость-2020”. Лыткарино. 22–23 сентября 2020. М.: НИИП, 2020. С. 146.
3. *Марфин В.А., Бойченко Д.В.* // Тр. 20-й Всерос. научн.-техн. конф. “Стойкость-2017”. Лыткарино. 6–7 июня 2017. М.: НИИП, 2017. С. 194.
4. *Peña-Fernandez M., Lindoso A., Entrena L., Garcia-Valderas M.* // IEEE Trans. 2020. V. NS-67. № 1. P. 126.
5. *Ахметов А.О., Бобровский Д.В., Калашников О.А., Некрасов П.В.* // Тр. Рос. научн.-техн. конф. “Радиационная стойкость электронных систем – Стойкость-2011”. Лыткарино. 7–8 июня 2011. М.: НИИП, 2011. С. 34.
6. *Кустов А.С., Пилипенко А.С., Сильянов Н.В.* // ВАНТ, Физика радиационного воздействия на радиоэлектронную аппаратуру. 2020. № 2. С. 24.
7. *Чумаков А.И.* // Микроэлектроника. 2006. Т. 35. № 3. С. 184.