Известия Гомельского государственного университета
имени Ф. Скорины, № 6(81), 2013

УДК 621.3.049.77–048.24:537.2

Планирование эксперимента по выявлению изменений в программном обеспечении микроконтроллеров с *flash*-памятью при воздействии электростатического разряда

Г.А. Пискун, В.Ф. Алексеев

Представлен новый подход к планированию эксперимента по технической диагностике микроконтроллеров с инсталлированным во встроенную *flash*-память программным обеспечением после воздействия электростатического разряда. Впервые предложен алгоритм, основанный на анализе целостности хранящегося во *flash*-памяти массива данных с применением специализированных хеш-функций. Показано, что предложенный алгоритм позволяет выявить потенциально ненадежные микроконтроллеры на стадии программирования.
Ключевые слова: микроконтроллер, электростатический разряд, хеш-функция.

A new approach to the planning of the experiment for technical diagnostics microcontroller with installed in the built-in *flash*-memory software after effects of electrostatic discharge. First an algorithm was proposed based on the analysis of the integrity of the stored in *flash*-memory dataset using specialized hash functions. It is shown that the proposed algorithm can detect potentially unreliable microcontrollers programming phase.
Keywords: microcontrollers, static discharge, hash function.

Введение. Обширная номенклатура современных микроконтроллеров (МК) с разнообразными функциональными возможностями создают разработчикам электронных средств, с одной стороны, достаточно хорошие условия для проектирования сложной конкурентоспособной аппаратуры различного назначения. С другой же стороны, осуществить эффективную защиту МК от внешних воздействий, особенно от такого деструктивного влияния как электростатический разряд (ЭСР), достаточно сложно, так как высокая степень микроминиатюризации компонентов, входящих в состав полупроводникового кристалла МК, влечет за собой повышение чувствительности к действию разрядов статического электричества. Таким образом, проблема обеспечения и оценки устойчивости МК в части функциональных и эксплуатационных характеристик к воздействию ЭСР приобретает особое значение [1]–[4].

Несмотря на значительное внимание, уделяемое в настоящее время методам оценки воздействия электростатических разрядов на МК, в них недостаточно глубоко рассматриваются процессы отказов, протекающие в таком наиболее значимом функциональном блоке микроконтроллеров, как *flash*-память. В свою очередь, это значительно осложняет проведение технической диагностики функционально сложной аппаратуры, построенной на базе МК, поскольку отказы могут происходить не только в части повреждений полупроводникового кристалла, но и в инсталлированном во встроенную *flash*-память МК программном обеспечении (ПО) [5], [6].

Таким образом, проведение изысканий в области оценки устойчивости МК с инсталлированным во встроенную *flash*-память ПО к воздействию ЭСР определяется фундаментальностью и сложностью проблемы, отсутствием адекватных моделей технической диагностики, а также алгоритмов оценки и проведения испытаний МК на устойчивость к воздействию ЭСР.

Учитывая существующую связь работоспособности МК и надежности электронных средств, исследования, направленные на решение задач повышения устойчивости микроконтроллеров к влиянию ЭСР, являются актуальными и представляют значительный интерес не только с научной, но и с практической точки зрения.

1. Исходная модель объекта диагностирования. Для выявления программных изменений в массиве данных, инсталлированном во встроенную *flash*-память микроконтроллера, вызванных влиянием разрядов статического электричества, наиболее оптимальным является совершенствование планирования эксперимента.

Планирование эксперимента – это процедура выбора числа и условий проведения опытов, необходимых и достаточных для решения поставленной задачи с требуемой точностью [4], [7].

Данный процесс обеспечивает оптимальное исследование разнообразных объектов в части:

– минимизации числа опытов и, следовательно, времени и затрат;

– реализации специальных планов эксперимента, предусматривающих одновременное варьирование всеми переменными;

– использования аппарата математической статистики, позволяющего формализовать многие действия экспериментатора и принимать обоснованные решения после каждой серии экспериментов.

На основании вышесказанного представим объект диагностирования, т.е. микроконтроллер, и все множество воздействующих факторов, определяющих работу исследуемого объекта, следующим образом (рисунок 1):

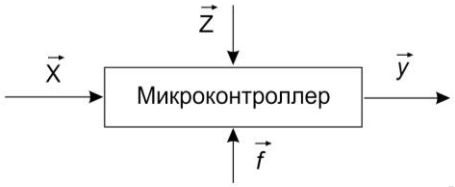

Рисунок 1 – Схема представления микроконтроллера для целей диагностирования

Одна часть входов системы является *p*-мерным вектором параметров МК $\vec{X}$, которые можно условно разделить на множество определяющих параметров (параметры, существенно влияющие на изменение выходных параметров МК) и множество неопределяющих параметров (параметры несущественно влияющие на изменение выходных параметров МК).

Другая часть входов представлена μ-мерным вектором входных воздействий $\vec{Z}$. Этот вектор представляет собой совокупность управляющих воздействий на микроконтроллер, каждое из которых характеризуется своими показателями.

Вместе с тем, на МК действует χ-мерный вектор дестабилизирующих воздействий $\vec{f}$, который определяется фактическими условиями эксплуатации исследуемого объекта.

На выходе МК наблюдается *m*-мерный вектор выходных параметров $\vec{y}$, который непосредственно зависит от параметров, поступающих с входов системы технической диагностики.

Связь входов и выходов диагностируемого микроконтроллера примет вид следующего уравнения (1) [4]:

$$y = W(x, z, f), \tag{1}$$

где W – оператор связи.

При этом, учитывая, что определяющим состоянием микроконтроллера является способность выполнять запрограммированные функции, под условием работоспособности рассматриваемой структурной единицы понимается выполнение совокупности следующих неравенств (2) [4]:

$$y_{j\min} \le y_j(x) \le y_{j\max}, \tag{2}$$

где $y_j(x)$ – функция работоспособности; y_{jmax}, y_{jmin} – наибольшее и наименьшее значение *j*-го параметра.

2. Методика проведения эксперимента с анализом используемых микроконтроллеров

Целью планирования эксперимента по выявлению изменений в инсталлированном программном обеспечении при воздействии на МК разрядов статического электричества является определение значения напряжения, при котором были выявлены изменения в массиве данных.

Достижение данной цели осуществлялось на основании реализации следующих задач:

1. Выполнение стирания встроенной *flash*-памяти микроконтроллеров с дальнейшей

записью и сверкой программного обеспечения с эталонной версией.

Эталонной версией программного обеспечения будем называть все или часть программ, процедур, правил и соответствующей документации системы обработки информации, относящихся к функционированию МК.

Учитывая то, что встроенная внутрисистемная электрически программируемая *flash*-память МК позволяет перепрограммировать память программ обычным программатором постоянной памяти, в эксперименте целесообразно использовать современный USB-программатор, например, *ChipProg-481* [8].

Для определения целостности данных при их записи и хранении во встроенной *flash*-памяти МК был произведен дополнительный расчет хеш-функций (MD5 и SHA-1), результаты которых представлены в таблице 1:

Таблица 1 – Полученные значения хеш-кодов для эталонного массива данных

Наименование хеш-функции	Хеш-код
MD5	74014bd69c9cf562409194ed5d867fdc
SHA-1	2d7d00af182c61fa166a8f3fd6fd830cf5eb78c6

2. Воздействие контактным разрядом статического электричества на МК.

На каждый контактный вывод МК производилось попеременно по 10 одиночных разрядов разной полярности с интервалом между последовательными одиночными разрядами равным 1 с. Длительность импульса составляет 0,7 ÷ 1 нс [9].

Разрядный наконечник испытательного генератора (ИГ) для осуществления контактного разряда ЭСР располагался перпендикулярно к поверхности контактных выводов МК, что позволяло улучшить повторяемость результатов проводимых испытаний (рисенок 3) [9].

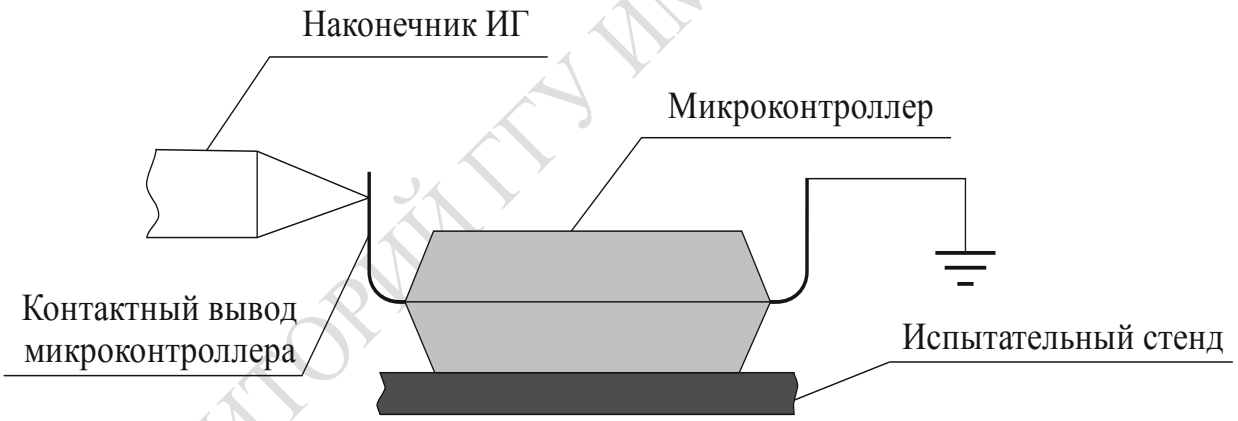

Рисунок 3 – Схема расположения разрядного наконечника испытательного генератора ЭСР

Первоначальное значение напряжения ЭСР (250 В) выбрано в соответствии с методом 502-1.1a [10]. Последующие значения напряжений воздействующих ЭСР составляли 500 В, 1 кВ, 2 кВ и 4 кВ. При данных значениях никаких изменений не было выявлено.

3. Ступенчатое повышение напряжения ЭСР.

Постепенное увеличение напряжения воздействующего разряда статического электричества на 0,1 кВ вызвано необходимостью получения более точных данных по отказам.

4. Сверка инсталлированного ПО во *flash*-памяти МК с эталонным.

Наиболее оптимальное проведение анализа целостности инсталлированного во встроенную *flash*-память массива данных возможно с помощью использования хеш-функций.

5. Определение степени повреждений ПО.

На данном этапе человек-оператор, осуществляющий диагностику МК, принимает решение о степени повреждения ПО и целесообразности дальнейшего использования.

Итоговый алгоритм имеет следующий вид (рисунок 4):

Рисунок 4 – Алгоритм анализа целостности массива данных

3. Экспериментальные результаты и их обсуждение. Для проведения эксперимента использовался МК типа Attiny 2313/V, который построен на AVR-усовершенствованной RISC-архитектуре и представляет собой восьмиразрядную микросхему с внутренней программируемой *flash*-памятью размером 2 Кб [11], [12].

В процессе стирания все ячейки памяти соответствуют значениям FF. Данная операция выполнялась в течении 3 мкс. Время записи массива данных размером 2 Кб составило 2 мкс. Использование встроенной в систему программатора функции сверки, позволило определить то, что программное обеспечение записано без каких-либо изменений.

Диагностика микроконтроллера типа Attiny 2313/V.

– напряжение ЭСР от 5,0 до 5,2 кВ.

Данное напряжение воздействующего разряда статического электричества не является стандартным, но его выбор обусловлен проведенным анализом технического описания на данный тип МК [11].

При воздействии на контактные выводы микроконтроллера с инсталлированным во встроенную *flash*-память программным обеспечением ЭСР не было выявлено никаких изменений в выполнении запрограммированных функций (рисунок 5).

Однако при осуществлении процесса стирания и записи было выявлено то, время записи массива данных размером 2 Кб составило 1 мин. 24 с. Также стоит отметить, что контрольные суммы записанного во *flash*-память программного обеспечения не соответствуют эталонному значению (табл. 2), что говорит о возникновении повреждений в структуре полупроводникового кристалла микроконтроллера.

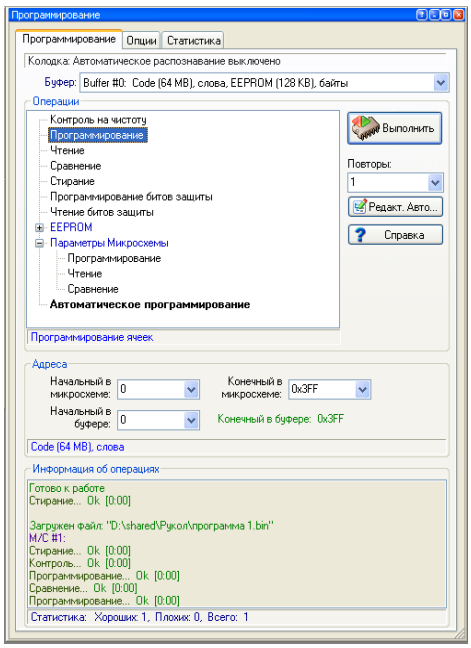

Рисунок 5 – Успешное проведение операций с микроконтроллером

Таблица 2 – Сравнение значений хеш-функций полученного ПО с эталонным

Наименование хеш-функции	Хеш-код	Результат
MD5	71e0129e33122b0393dcb329112d567d	Полученное
	74014bd69c9cf562409194ed5d867fdc	Эталонное
SHA-1	24c8b30ac252c92813c4a0e65e22938990f747e2	Полученное
	2d7d00af182c61fa166a8f3fd6fd830cf5eb78c6	Эталонное

Из анализа хеш-кодов видно, что полученные и эталонные значения расходятся. Таким образом, начальным значением напряжения, при котором начинается изменение в инсталлированном во встроенную *flash*-память МК программном обеспечении, является 5,0 кВ.

– напряжение ЭСР – 5,3 кВ.

После воздействия на контактные выводы МК разрядом статического электричества напряжением 5,3 кВ было осуществлено обращение к встроенной *flash*-памяти МК с помощью программатора. Однако при этом были выявлены значительные повреждения, не позволяющие проведение каких-либо операций (рисунок 6).

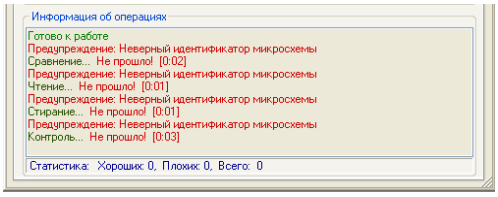

Рисунок 6 – Проведение операций со встроенной *flash*-памятью МК невозможно

Учитывая то, что из памяти микроконтроллеров невозможно было считать какую-либо информацию, то снять контрольные суммы и сверить их значения с эталонными значениями также было невозможно.

– напряжение ЭСР – 5,4 кВ и выше.

На этапе функционального контроля исследуемых МК провести какие-либо операции было невозможно, что, в свою очередь, обусловлено полной утратой работоспособности [13].

На основании полученных результатов вследствие проведения эксперимента построим графическую зависимость проявления повреждений в массиве данных, хранящемся во встроенной *flash*-памяти МК, после воздействия разрядов статического электричества различных номиналов (рисунок 7).

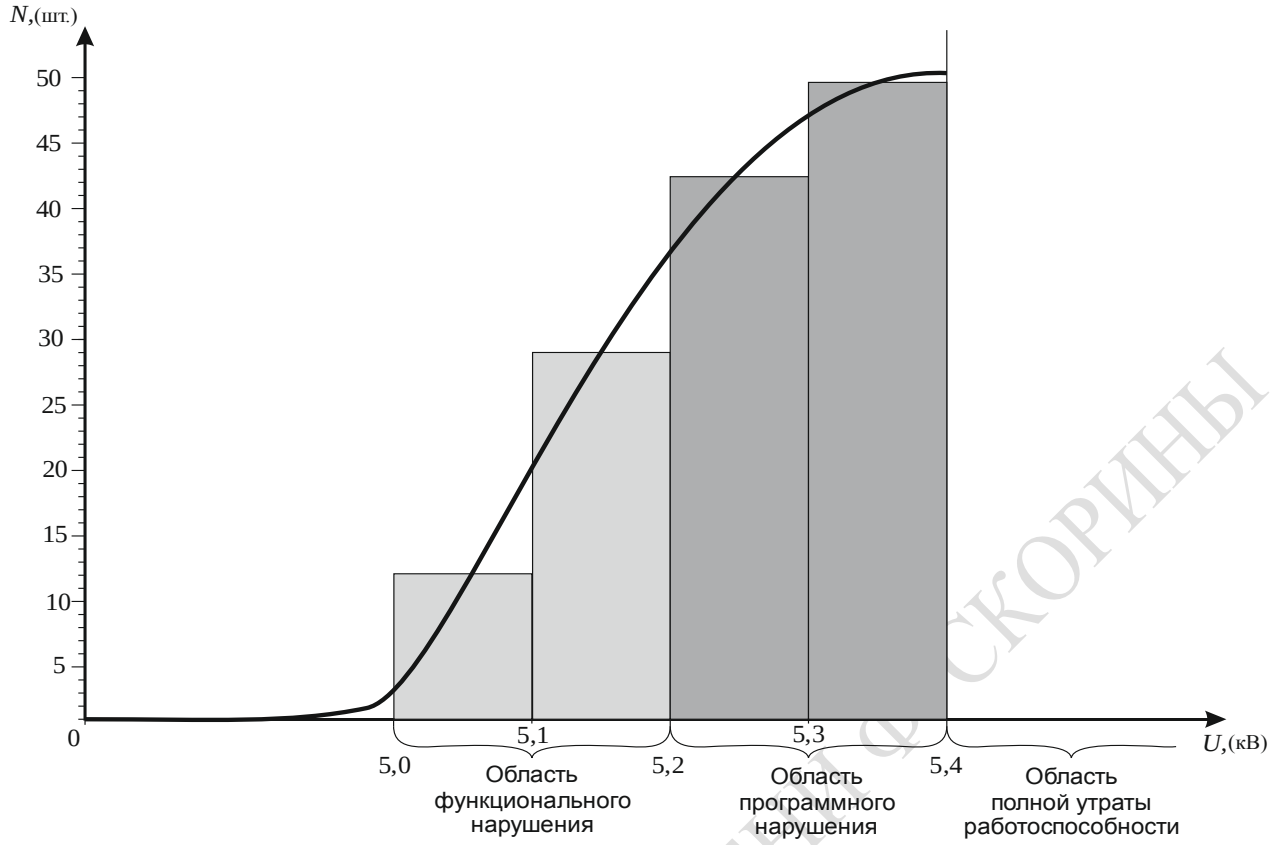

Рисунок 7 – Диаграмма проявления повреждений массива данных

Из рисунка видно, что экспериментально полученные данные по количеству микроконтроллеров (*N*), в которых были выявлены нарушения в инсталлированном массиве данных и представленные в виде интервалов значения напряжения (*U*) воздействующего разряда статического электричества, можно описать нормальным законом распределения.

Заключение. В результате проведенного анализа микроконтроллеров с инсталлированным во встроенную *flash*-память программным обеспечением с помощью специализированных хеш-функций было выявлено, что нарушения в массиве данных наступает значительно раньше, чем катастрофическое повреждение самого МК [14].

Результаты экспериментов позволяют создавать и интегрировать в процесс производства и эксплуатации современных микроконтроллеров вероятностные показатели, которые позволят осуществить наиболее точное прогнозирование потенциально ненадежных МК на этапе инсталляции программного обеспечения.

Литература

1. Горлов, М.И. Электростатические заряды в электронике / М.И. Горлов, А.В. Емельянов, В.И. Плебанович. – Минск : Белорусская наука, 2006. – 295 с.

2. Кечиев, Л.Н. Защита электронных средств от воздействия статического электричества / Л.Н. Кечиев, Е.Д. Пожидаев // М. : Издательский Дом «Технологии», 2005. – 352 с.

3. Хабигер, Э. Электромагнитная совместимость. Основы ее обеспечения в технике / Э. Хабигер ; пер. И.П. Кужекина. / под ред. Б.К. Максимова. – М. : Энергоатомиздат, 1995. – 304 с.

4. Портнягин, Н.Н. Теория и методы диагностики судовых электрических средств автоматизации / Н.Н. Портнягин, Г.А. Пюкке. – Петропавловск-Камчатский : КамчатГТУ, 2003. – 117 с.

5. Алексеев, В.Ф. Методика испытания микроконтроллеров на чувствительность к электростатическим разрядам / В.Ф. Алексеев, Н.И. Силков, Г.А. Пискун, А.Н. Пикулик // Доклады БГУИР. – 2011. – № 5 (59). – С. 5–12.

6. Алексеев, В.Ф. Методика оценки устойчивости микроконтроллеров к воздействию разрядов статического электричества при ступенчатом повышении напряжения / В.Ф. Алексеев, Г.А. Пискун // Вестник Рязанского государственного радиотехнического университета. – 2012. – № 2 (40). – С. 34–40.

7. Адлер, Ю.П. Планирование эксперимента при поиске оптимальных условий. Программное введение в планирование эксперимента / Ю.П. Адлер, Е.В. Маркова, Ю.В. Грановский // М. : Наука, 1976 – 144 с.

8. USB программатор ChipProg-481 [Электронный ресурс].– Режим доступа: http://www. chipdip. ru. Дата доступа 20.07.2013.

9. Электромагнитная совместимость. Часть 4–2. Методы испытаний и измерений. Испытания на устойчивость к электростатическим разрядам : СТБ МЭК 61000-4-2-2006. – Введ. 08.12.06. – Минск : Межгос. совет по стандартизации, метрологии и сертификации : Белорус. гос. ин-т стандартизации и сертификации, 2006. – 27 с.

10. Микросхемы интегральные. Методы испытаний. Методы электрических испытаний. Часть 7. : ОСТ 11 073.013-2008. – Введ. 01.01.09. – Российская Федерация : Госстандарт России, 2009. – 35 с.

11. Datasheet Attiny 2313/V [Электронный ресурс]. – 2009. – Режим доступа: http://www.datasheet.su. Дата доступа 22.07.2013.

12. Бродин, В.Б. Системы на микроконтроллерах и БИС программируемой логики. / В.Б. Бродин, А.В. Калинин // М. : Издательство ЭКОМ, 2002. – 400 с.

13. Пискун, Г.А. Устойчивость радиоэлектронного оборудования на базе микроконтроллеров к электростатическим разрядам / Г.А. Пискун, В.Ф. Алексеев, А.Н. Пикулик // Стандартизация. – 2012. – № 1–2012. – С. 37–39.

14. Пискун, Г.А. Контроль функционирования микроконтроллеров при воздействии электростатического разряда / Г.А. Пискун, В.Ф. Алексеев // Доклады БГУИР. – 2012. – № 6 (68). – С. 12–18.

Белорусский государственный университет
радиоэлектроники и информатики

Поступила в редакцию 16.01.2013