Розглянуті эффективні способи дії на напівпровідникові електронні носії інформації. Визначений наибільш перспективний комбінований метод знищення інформації, що забесчує одночасну реализацію декількох способів дії. Розглянутий пристрій для знищення інформації з носієм на основі мікросхем с энергонезалежною пам'яттю, в якому запропонований метод реалізований. Результати проведених випробувань разробленого пристрою підтвердили надійність стирання інформації с флеш носіїв

Ключові слова: комбінований метод, флеш, электромагнітне поле, напівпровідниковий носій, СВЧ поле

Рассмотрены эффективные способы воздействия на полупроводниковые электронные носители информации. Определен наиболее перспективный комбинированный метод уничтожения информации, обеспечивающий одновременную реализацию нескольких способов воздействия. Рассмотрен прибор для уничтожения информации с носителей на основе микросхем с энергонезависимой памятью, в котором предложенный метод реализован. Результаты проведенных испытаний разработанного прибора подтвердили надежность стирания информации с флеш носителей

Ключевые слова: комбинированный метод, флеш, электромагнитное поле, полупроводниковый носитель, СВЧ поле

УДК 621.318.12

КОМБИНИРОВАННЫЙ МЕТОД УНИЧТОЖЕНИЯ ИНФОРМАЦИИ С ПОЛУПРОВОДНИКОВЫХ НОСИТЕЛЕЙ С ЭНЕРГОНЕЗАВИСИМОЙ ПАМЯТЬЮ

Б.В. Хлопов
Кандидат технических наук, доцент, начальник отдела*
Контактный тел. (499) 263-96-25
E-mail: hlopovu@yandex.ru
Ю.С. Бондарев
Доктор военных наук, первый заместитель генерального директора*
Контактный тел.: (495) 267-43-93
E-mail: 208_otd@mail.ru
А.В. Шпак
Кандидат технических наук, начальник научно-технического отдела*
ФГУП «ЦНИРТИ им.академика А.И. Берга»
Контактный тел. (499) 267-53-07
E-mail: hlopovu@yandex.ru
М.В. Фесенко
Кандидат технических наук, заместитель начальника отдела*
Контактный тел. (499) 263-95-38
E-mail: hlopovu@yandex.ru
*ФГУП «ЦНИРТИ им. академика А.И. Берга»
ул. Новая Басманная, 20, г. Москва, Россия, 105066

1. Введение

Полупроводниковые носители имеют одну особенность, заключающуюся в отсутствии прямых методов контроля, состояния каждой ячейки памяти после стирания информации.

Информация, содержащаяся в полупроводниковом устройстве, при контроле обнаруживается путем приложения напряжения к затвору полупроводникового элемента, значение которого лежит между двумя возможными пороговыми значениями напряжений. В одном состоянии элемент (транзистор) проводит ток, в то время как в другом не проводит, заперт. В приборах хранения заряда с изолированным затвором осуществляется двумя способами. Один способ основан на хранении заряда в проводящем или полупроводящем слое, окруженном диэлектриком, обычно окисью кремния [1] с плавающим затвором [2, 3]. Другой тип приборов, основан на хранении заряда на дискретных центрах (ловушках) соответствующего диэлектрического слоя.

Эти устройства обычно называют приборами захвата [4, 5].

Для обеспечения контроля состояния каждой ячейки и доступа к флэш-памяти необходим программно-аппаратный комплекс, контроллер - посредник между хостом и устройствами на шине. Программные функции возложены на операционную систему.

Наиболее распространенной операционной системой, в которой реализована поддержка доступа к флэш-памяти в полном объеме, является Windows.

Недостатком этого прямого метода контроля стирания записи с устройств энергонезависимой памяти, флэш-памяти, является низкая энергетическая эффективность. Для стирания информации и контроля стирания информации необходимо иметь программно-аппаратный комплекс, операционную систему, определенный тип доступа к памяти, который определяет относительно большое время стирания информации, возможность восстановления информации. Использование программно-аппарат-

ных средств ПЭВМ предопределяет возможность несанкционированного доступа к информации, при целенаправленном уничтожении информации с носителя, что чрезвычайно актуально. Важность данной проблемы возрастает для случаев специальных документов, которые должны быть сохранены или гарантировано и максимально оперативно уничтожены. Достоверность уничтожения информации с полупроводниковых носителей на основе микросхем с энергонезависимой памятью (флеш – памятью) в устройствах экстренного стирания информации подтверждается измеряемыми параметрами встроенной системой контроля (ВСК).

2. Методы воздействия на полупроводниковые носители на основе микросхем с энергонезависимой памятью (флеш – памятью)

В процессе исследований установлено, что из всех возможных методов воздействий наиболее эффективными методами воздействия на полупроводниковые электронные носители информации выделены:

- воздействия на носитель информации электромагнитным полем;
- воздействие магнитным импульсом высокой напряженности;
- воздействие коротким импульсом СВЧ поля;
- кратковременное воздействие электрическим импульсом высокого напряжения на интерфейсные выводы устройства хранения информации.

При разработке и изготовлении устройств экстренного уничтожения информации на микросхемах с неоднородным полупроводниковым носителем с энергонезависимой памятью использовали комбинированный вариант, совмещающий в себе два или несколько методов стирания при одновременном воздействии. В результате проведенных исследований, подробного анализа различных конструктивных и энергетических возможностей составных частей устройства экстренного уничтожения информации, обеспечивающих создание электромагнитного поля и воздействующих факторов, с характеристиками, гарантирующими экстренное уничтожение записанной информации на полупроводниковом носителе информации предложены методы косвенной оценки. Оценка проведена по электронным, электрическим, частотным и конструктивным параметрам так, как с высоким быстродействием в реальном масштабе времени в малогабаритном переносном устройстве экстренного уничтожения информации с полупроводниковых носителей этим методом эффективный контроль возможно реализовать с меньшими энергетическими и экономическими потерями и проще конструктивно чем прямым измерением основных контролируемых параметров.

3. Приборы для уничтожения информации с носителей на основе микросхем с энергонезависимой памятью

В разработанных и созданных опытных образцах приборов для экстренного уничтожения информации [6] на носителях информации с энергонезависимой памятью использовали как индивидуальные так и комбинированные способы, совмещающие в себе методы воздействия магнитными и короткими электромагнитными импульсами с другими эффективными методами.

В устройстве стирания [7] реализован способ стирания записанной на микросхеме с неоднородным полупроводниковым носителем информации с энергонезависимой памятью, состоящий в том, что на микросхему, на управляющий затвор в течении 1,5 мс, подают номинальные напряжения питания и одновременно проводниках микросхемы, возбуждают токи Фуко интенсивностью не менее 60 мА с помощью облучения проводников микросхемы двумя ортогональными переменными синусоидальными магнитными полями под углами с разными значениями.

В приборе [8] реализован способ при котором на полупроводниковый носитель через шину USB воздействуют сформированными короткими импульсами с определенным алгоритмом и количеством циклов, а по окончании генерации импульсов воздействуют импульсным током значением 2,0 А, образованным за счет разряда накопленного напряжения до 400 В на накопителях энергии.

Стирание информации в полости полеобразующей системы устройств [9,10] осуществляется путем воздействия суммарным импульсным магнитным полем образованным магнитными полями с векторами напряженности направленными под различными углами (a,b,s).

Техническая сущность устройства стирания информации с полупроводниковых носителей [11] заключается в подаче на микросхему на управляющий затвор напряжения и в возбуждении в ее проводниках токов Фуко с одновременным воздействием энергией тепла, излучаемой отражателем. Учитывая, что в разработанных и созданных опытных образцах приборов, для экстренного уничтожения информации на носителях с энергонезависимой памятью, используются в основном комбинированные способы уничтожения информации, выбор остановлен на косвенных методах контроля как наиболее экономичных и обеспечивающих необходимую точность.

4. Описание компоновки исследуемого изделия экстренного стирания информации с электронных полупроводниковых носителей информации

Изделие представляет собой конструктивно законченное устройство, в котором предусмотрено размещение флеш-накопителей различного типа. В конструкции изделия размещены следующие модули и элементы: полеобразующая система; накопитель энергии; источник вторичного электропитания; устройства управления, запуска и обеспечения функционирования изделия; встроенная система контроля (ВСК) работоспособности изделия; генератор коротких импульсов; устройство обеспечения теплового режима; устройство заряда аккумулятора; аккумулятор; ЗИП [12]. На рис. 1 приведена функциональная схема встроенной системы контроля для изделия экстренного стирания информации с электронных полупроводниковых носителей информации.

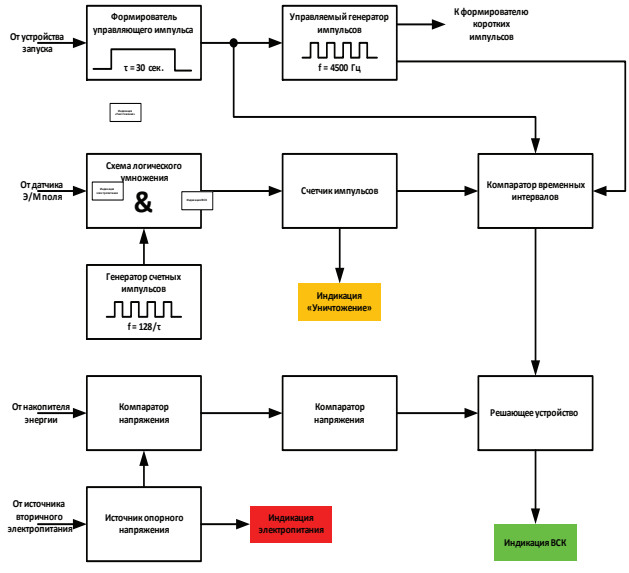

Рис. 1. Функциональная схема встроенной системы контроля

Встроенная система контроля выдает информацию о функционировании изделия при каждом отдельном запуске. Система встроенного контроля работает в ключевом режиме.

Для проверки принятого решения применение комбинированного уничтожения информации проведена оценка стирания информации методом косвенного контроля.

Создано устройство стирания информации с полупроводниковых носителей. Оно состоит из трех каналов, обеспечивающих комбинированное уничтожение информации. В схеме устройства не приведены блоки, некритичные для процесса уничтожения информации, а также заменяемые ручной регулировкой и лабораторными приборами (датчик тока, схема автоподстройки частоты). Кроме того, устройство отличается упрощенной конструкцией в целях возможности изготовления без применения специального оборудования. Устройство разделено на несколько печатных плат: источник вторичного электропитания; фильтр; задающий генератор и схема согласования; генератор коротких импульсов; схема управления; встроенная система контроля; датчик электромагнитного поля. Остальные элементы соединены объемным монтажом. Устройство имеет алюминиевый корпус. В корпусе имеются: окно загрузки носителя информации, элементы управления и кабель питания. На переднюю панель вынесены элементы управления: выключатель питания; кнопка запуска, индикации питания, готовности, встроенной системы контроля. На рис. 2 показан источник вторичного электропитания. Большая часть элементов располагается на печатной плате. Фильтр источника питания расположен на отдельной плате. Транзисторы установлены на радиаторы. Для улучшения теплопроводности используется паста КПТ-8.

Управляемый задающий генератор, схема согласования, коммутатор и фильтр находятся на минимальном расстоянии друг от друга для уменьшения паразитной индуктивности, соединяющих проводов (рис. 3). Коммутатор изготовлен по мостовой схеме на транзисторах MOSFET и блока конденсаторов. Транзисторы установлены на радиаторы, для улучшения теплопроводности с использованием пасты КПТ-8. Фильтр закреплен на основании.

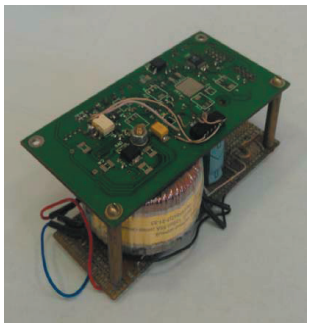

Рис. 2. Источник вторичного электропитания

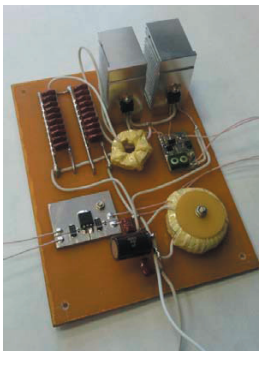

Рис. 3. Управляемый задающий генератор импульсов, схема согласования, коммутатор и фильтр

Генератор коротких импульсов показан на рис. 4. Все элементы расположены на печатной плате. Используется поверхностный монтаж. Выходной сигнал поступает на облучатель по коаксиальному кабелю.

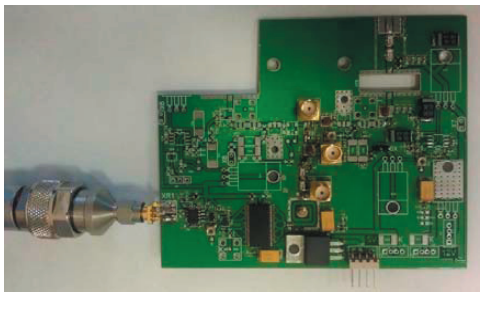

Рис. 4. Генератор коротких импульсов

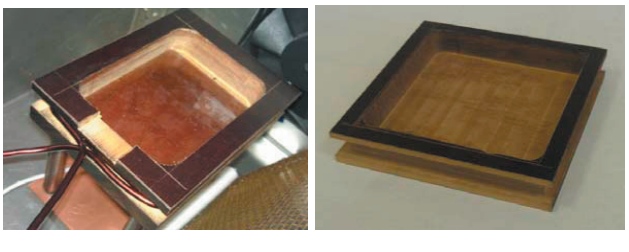

Рис. 5. Полеобразующая система (рисунок справа - рабочая камера, рассчитанная под SSD)

5. Результаты испытаний составных частей устройства

В разработанный стенд для испытаний устройства введены приборы и оборудование: осциллограф Tektronix TDS 2022B; осциллограф TRIM TMR 8120; токосъемник измерительный ТИ2-3; мультиметр APPA 205; лабораторный источник питания Mastech HY3020. Напряжение питания при испытаниях составляло 90 В, что меньше номинального, так как используются лабораторные источники питания. Это необходимо учитывалось при анализе результатов измерения.

Испытание канала воздействия на носитель информации электромагнитным полем с частотой 400...500 кГц

Поскольку создаваемое электромагнитное поле сложно измерить непосредственно вследствие наведения мощных индукционных токов и сильного нагрева проводящих элементов внутри полеобразующей системы, используется косвенный метод измерения. Оцениваемым параметром является ток в полеобразующей системе, расчетное значение которого составило 85 А. На рис. 6 приведена функциональная схема датчика электромагнитного поля.

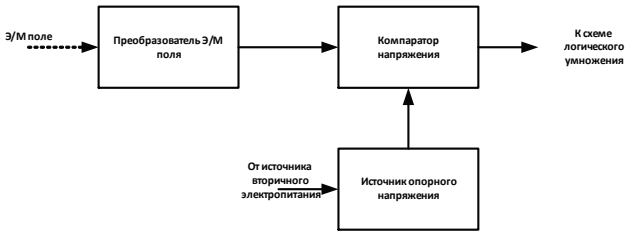

Рис. 6. Функциональная схема датчика электромагнитного поля

Для измерений при испытаниях используется токосъемник ТИ2-3, охватывающий подводящий провод полеобразующей системы. Напряжение, наводимое в токосъемнике, измеряется осциллографом TDS 202-2B. Поскольку полеобразующая система представляет собой резонансный контур, требуется подстройка частоты генератора для достижения максимальной амплитуды тока.

Также вследствие резонанса ток через полеобразующую систему является синусоидальным. Форма тока показана на рис. 7.

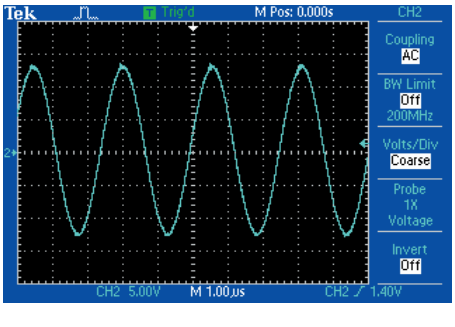

Рис. 7. Осциллограмма тока в полеобразующей системе

При напряжении питания 90 В получены следующие результаты измерений частоты и напряжения сигнала, снимаемого с токосъемника: F = 422 кГц, U = =214 В. Полученная с помощью осциллографа амплитуда напряжения пересчитывается в ток, протекающий в полеобразующей системе.

Напряжение в децибелах относительно 1 мкВ рассчитывается по формуле:

$$U_0 = 20 \cdot \lg\left(\frac{U_{изм}}{1 \cdot 10^{-6}}\right), \quad (1)$$

где $U_{изм}$ – напряжение, измеренное осциллографом.

Тогда ток в децибелах относительно 1 мкА:

$$I_0 = U_0 + K,$$

где K – коэффициент калибровки токосъемника, значения которого берутся из свидетельства аттестации токосъемника.

Для частоты 420 кГц K ≈ 1,5.

Абсолютное значение тока в полеобразующей системе:

$$I = 10^{\frac{I_0}{20}} \cdot 10^{-6}. \quad (2)$$

Полученный в ходе расчетов ток составил 89,9 А.

Испытание канала уничтожения информации импульсом высокого напряжения

Поскольку длительность импульса сильно зависит от уничтожаемого носителя информации, контролю подвергается напряжение на накопителе энергии, непосредственно связанное с величиной запасенной энергии по формуле:

$$W = \frac{C \cdot U^2}{2}. \quad (3)$$

Моделирование заряда накопителя энергии проводилось с помощью программы Micro-Cap 9. График заряда показан на рис. 8.

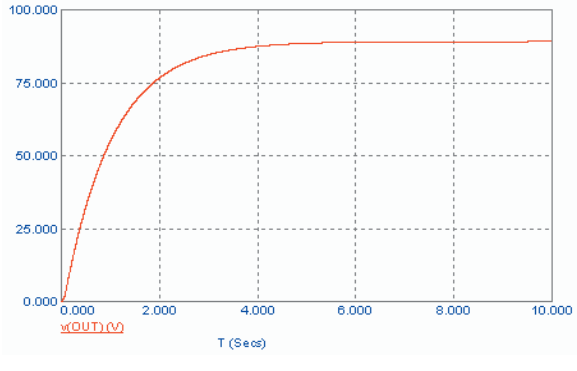

Рис. 8. График заряда накопителя энергии

По графику видно, что накопитель при энергии заряжается до напряжения 89 В за 7 с и далее это напряжение практически не изменяется. При проведении испытаний было измерено напряжение на накопителе энергии через 20 с после включения питания. Измеренное напряжение составило 87,8 В.

Испытание канала уничтожения информации коротким импульсом СВЧ поля

При испытаниях с помощью осциллографа TDS2022 B были получены в контрольных точках сигналы для оценки формы импульсов, а также измерена амплитуда выходного импульса. Осциллограммы сигналов в контрольных точках показаны на рис. 10–15. На вход генератора подаются запускающие импульсы с частотой 100 кГц и амплитудой около 1 В. Осциллограмма сигнала показана на рис. 9.

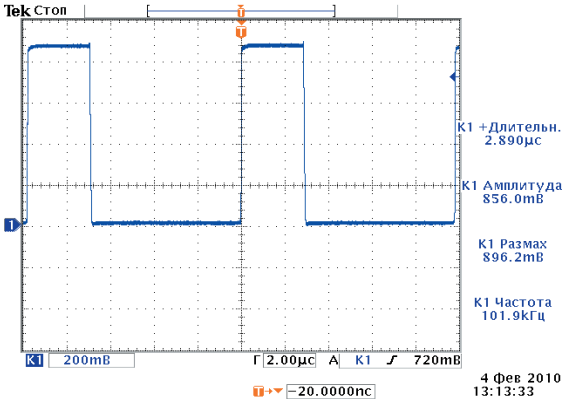

Рис. 9. Осциллограмма запускающих импульсов

Измеренные параметры запускающих импульсов приведены в табл. 1.

Таблица 1

Параметр	Значение	Единица измерения
Частота запускающих импульсов	101,8	кГц
Длительность запускающих импульсов	2,89	мкс
Амплитуда запускающих импульсов	0,896	В

Для оценки правильности работы устройства и необходимой настройки снята осциллограмма на выходе компаратора (рис. 10). Форма и параметры импульсов практически не изменились, значительно уменьшился уровень шумов.

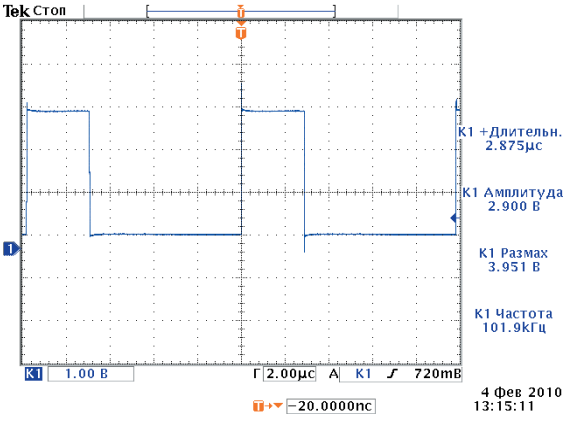

Рис. 10. Осциллограмма сигнала на выходе компаратора

Формирователь импульсов вырабатывает короткие импульсы с большой скважностью (рис. 11).

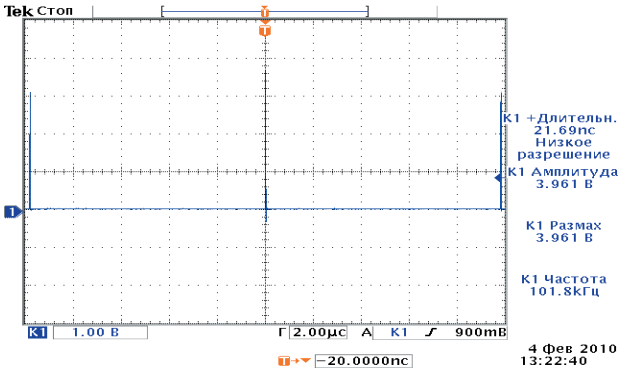

Рис. 11. Осциллограмма сигнала на выходе формирователя импульсов с сохранением временного масштаба

Длительность импульса на выходе формирователя импульсов устанавливается с помощью настроечного резистора R равной 20 нс (рис. 12).

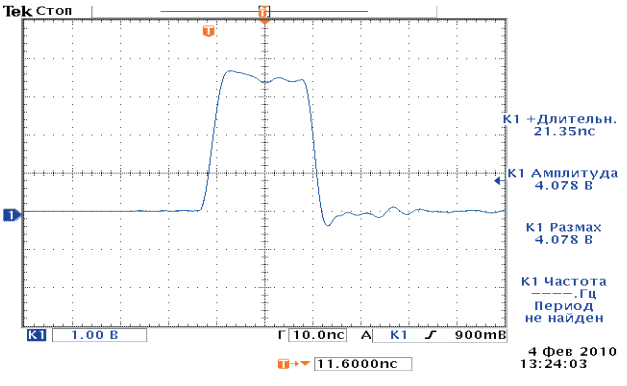

Рис. 12. Осциллограмма сигнала на выходе формирователя импульсов

На выходе формирователя коротких импульсов создается короткий импульс отрицательной полярности с большой амплитудой (рис. 13).

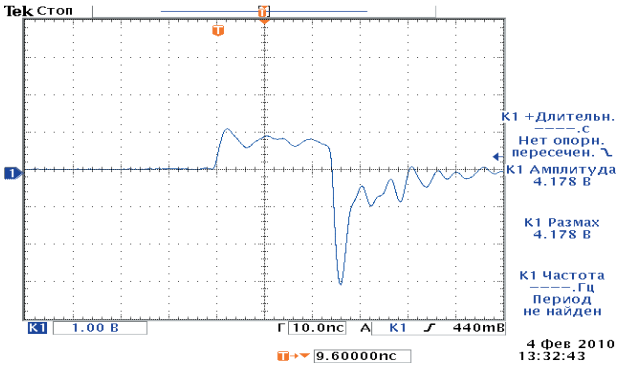

Рис. 13. Осциллограмма сигнала на выходе формирователя коротких импульсов

Полученный короткий импульс проходит через фильтр и усиливается выходным усилителем. Амплитуда сигнала, полученная в результате расчетов должна быть не менее 5 В. Осциллограмма импульса на выходе генератора, полученная с помощью осциллографа TMR показана на рис. 14. Измеренная амплитуда импульса примерно равна 5,5 В (с учетом аттенюатора).

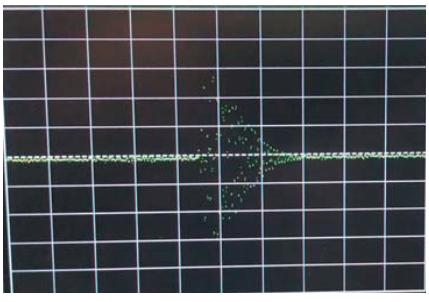

Рис. 14. Осциллограмма сигнала на выходе усилителя

6. Выводы

1. Полученные в ходе измерений осциллограммы соразмерны с расчетными. Значения частоты, замеренные при испытаниях отличается от расчетных на 4,5%, что может быть вызвано разбросом параметров конденсаторов контура и индуктора полеобразующей системы. Полученное значение тока в полеобразующей системе больше расчетного на 5,7% и находится в допустимых пределах.

2. Измеренное в ходе проведения испытаний напряжение составило 87,8 В, что на 1,3% меньше расчетного значения. Такое отклонение может быть вызвано током утечки конденсатора и вполне допустимо.

3. Амплитуда импульса на выходе генератора больше расчетной на 10%. Частота запускающих импульсов незначительно отличается от расчетной (на 1,8%).

4. Анализ результатов и полученных значений измерений, в ходе проведения испытаний позволяет сделать вывод, что результаты соответствуют расчетным, удовлетворяют общим конструктивным требованиям и свидетельствуют о правильной работе устройства уничтожения информации с полупроводниковых носителей с энергонезависимой памятью.

5. Достоверность и надежность уничтожения информации с полупроводниковых носителей на основе микросхем с энергонезависимой памятью (флеш – памятью) в устройствах экстренного стирания информации с высокой степенью вероятности косвенным методом подтверждается измеряемыми параметрами ВСК.

6. Разработанные методики испытаний использованы при испытаниях изготавливаемых устройств в системах встроенного контроля. Работа выполнена при поддержке РФФИ № 11-07-00301.

Литература

1. Аваев, Н.А. Электронные приборы [Текст] / Аваев Н.А., Шишкин Г.Г. // М.: Изд-во МАИ, 1996. – 544 с.: ил.
2. D. Frohman-Bentchkowsky, “Memory behaviour in a floating gate avalanche injection MOS (FAMOS) structure,”// Appl. Phys. Lett., vol. 18, 1971, p.332.
3. Балякин, И.А. Приборы с переносом заряда в радиотехнических устройствах обработки инфорамации [Текст] / И.А. Балякин и др. // М.: Радио и связь, 1987. – 176 с.: ил.
4. Секен, К. Приборы с переносом заряда. Перевод с английского [Текст] / К. Секен, М. Томпсет // М.: Мир, 1978 с., ил.
5. Гуляев, Ю.В. “Нано-микросистемная техника” [Текст] / Гуляев Ю.В., Лобанов Б.С., Митягин А.Ю., Хлопов Б.В., Фесенко М.В. // 2009 г., № 11, С.42-46.
6. Митягин, А.Ю. Аппаратура для уничтожения информации с современных носителей [Текст] / А.Ю. Митягин, Б.В Хлопов // Palmarium Academic Publishing (LAP LAMBERT Academic Publishing CmbH Co. KG, P. 168.
7. Митягин А.Ю., Хлопов Б.В., Фесенко М.В., Крутов М.М. / Патент на изобретение №2323491 от 27.04.2008г. (приоритет от 16.05.2006г). Бюл. №12.
8. Митягин А.Ю., Лобанов Б.С., Хлопов Б.В., Фесенко М.В., Кузминых А.С. / Патент на изобретение №2428754 от 10.09.2011г. (приоритет от 02.03.2010г). Бюл. №25.
9. Хлопов Б.В., Фесенко М.В. / Патент на изобретение №2346345 от 10.02.2009г. (приоритет от 26.04.2007г). Бюл. №4.
10. Фесенко М.В., Хлопов Б.В. / Патент на полезную модель №60255 от 10.01.2007г. (приоритет от 26.09.2007г). Бюл. №1.
11. Хлопов Б.В., Лобанов Б.С., Бондарев Ю.С., Фесенко М.В., Дьяков М.С. / Патент на изобретение №105510 от 10.06.2011г. (приоритет от 27.12.2010г). Бюл. №16.

Abstract

Now the industry of the different countries and the wide nomenclature of data carriers, based on chips of flash, memory are issued. These mobile data carriers turned into portable computers and servers. At the certain minuses connected with a resource of work, they are used in professional communication systems since they are especially steady against external influence. The use of hardware-software means of PEVM predetermines possibility of unauthorized access to information on semi-conductor carriers, which is an actual problem. Importance of this problem increases for cases of special documents, which should be kept or guaranteed and are most operatively destroyed from semi-conductor carriers with non-volatile memory. The use of the process combining two and more methods of deleting of information in real time with simultaneous built-in control increases reliability of deleting of information. The offered method effectively could be used in devices of emergency deleting of information in communication systems.

Keywords: *combined method, indirect control, semi-conductor data carriers, (flash – memory), built-in monitoring system, device of transformation of tension, device of correction of a charge; device of accumulation of energy; shaper of impulses of management*