A. M. Korotin

Novel Kinds of Random Access Memory and New Vulnerabilities of Computer Aids based on Them

Keywords: Random Access Memory (RAM), non-volatile RAM, MRAM, FeRAM, PCM, vulnerability of novel RAM, protection of computer aids based on the non-volatile RAM

The article discusses vulnerabilities of computer aids based on existing RAM and mechanisms for restricting exploitation of such vulnerabilities. In addition, the article discusses features and work methods of different RAM.

А. М. Коротин

ПЕРСПЕКТИВНЫЕ ВИДЫ ПАМЯТИ С ПРОИЗВОЛЬНЫМ ДОСТУПОМ И НОВЫЕ УЯЗВИМОСТИ СВТ НА ИХ ОСНОВЕ

Компьютерная память в составе вычислительной системы используется для хранения данных. По способу доступа все типы памяти можно разделить на две группы: память с произвольным доступом (RAM — Random Access Memory) и память с последовательным доступом (SAM — Sequential Access Memory). При использовании в средствах вычислительной техники (СВТ) памяти с произвольным доступом возможно напрямую обратиться к случайно выбранной ячейке, в то время как при работе с памятью последовательного доступа для чтения или записи информации в n-ю ячейку необходимо предварительно обратиться к n — 1 ячейке памяти. Такие различия в моделях доступа к информации оказывают влияние и на быстродействие памяти: память с произвольным доступом обеспечивает значительно меньшие временные затраты на чтение и запись информации. Как правило, RAM является энергозависимой памятью и сохраняет информацию лишь при подаче электроэнергии, в то время как SAM является энергонезависимой и сохраняет информацию даже в отсутствие электропитания.

В данной статье производится анализ уязвимостей СВТ на основе существующих видов памяти с произвольным доступом и возможных механизмов блокирования эксплуатации таких уязвимостей. Вначале предлагается проанализировать характеристики и принципы работы известных видов RAM, далее изучить возможные уязвимости СВТ на их основе и в заключение выработать механизмы защиты от эксплуатации таких уязвимостей.

В существующих видах RAM можно выделить две основные группы: RAM, повсеместно используемые на сегодняшний день, и новые перспективные виды RAM, которые уже имеются в виде опытных образцов, но еще слабо распространены в мире. Основной целью разработок перспективных видов памяти с произвольным доступом является объединение лучших сторон RAM первой группы и создание так называемой «универсальной памяти», которая являлась бы энергонезависимой, обеспечивала высокое быстродействие, малое энергопотребление и имела высокую плотность размещения ячеек. К первой группе относятся такие виды памяти, как DRAM, SRAM и flash, ко второй — FRAM, MRAM и PCM. Далее подробно опишем каждую из перечисленных здесь видов RAM.

Распространенные виды RAM

DRAM

Динамическая память с произвольным доступом, или DRAM (Dynamic Random Access Memory), является видом полупроводниковой энергозависимой памяти. DRAM состоит из элементарных ячеек памяти, каждая из которых содержит конденсатор, сохраняющий заряд, и

управляющий транзистор. Процесс записи информации в ячейку DRAM заключается в зарядке конденсатора, чтение — его разрядка. Процесс чтения информации из ячейки DRAM является деструктивным и требует последующей регенерации данных, что увеличивает энергопотребление DRAM. Наличие заряда в конденсаторе соответствует логической единице, отсутствие заряда — логическому нулю.

Так как конденсатор может сохранять заряд только в течение небольшого периода времени — порядка 20 мс [1], необходимо постоянно обновлять хранящийся в конденсаторе заряд во избежание потери информации. Такой процесс обновления содержимого ячеек называется регенерацией памяти. В течение времени, которое называется шагом регенерации, в DRAM полностью перезаписывается строка ячеек. Таким образом, обновление всех строк памяти происходит за несколько миллисекунд (примерно 8—64 мс) [2]. Такой динамический принцип поддержания заряда в конденсаторе и дал название данному типу памяти.

Площадь любой ячейки памяти произвольного доступа, не только DRAM, зависит от числа используемых полупроводниковых элементов, их размеров, особенностей соединения элементов между собой и их подсоединения к линиям связи. Размеры полупроводниковых элементов определяются используемым технологическим процессом. На сегодняшний день размеры полупроводниковых элементов, используемых в DRAM, достигли значения 20 нм [3]. Обозначим через параметр F размер используемых полупроводниковых элементов. Тогда площадь одной ячейки DRAM будет определяться формулой $8F^2$ [4]. Изменения архитектуры ячейки, порядка соединения элементов между собой и с линиями связи позволили уменьшить площадь ячейки DRAM сначала до величины $6F^2$, а затем и $4F^2$. Таким образом, на сегодняшний день площадь ячейки DRAM может достигать 0,0016 нм^2. Это позволяет достичь плотности размещения элементов, сравнимой с NAND-flash-памятью, при том, что скорость работы в десятки раз выше.

SRAM

Статическая память с произвольным доступом, или SRAM (Static Random Access Memory), аналогично динамической RAM, является видом полупроводниковой энергозависимой памяти, однако, в отличие от DRAM, не требует процесса регенерации памяти. Данное свойство SRAM объясняется строением ее ячеек памяти. Каждая ячейка представляет собой триггер — логическое устройство, способное длительное время находиться в одном из двух устойчивых состояний и переходить из одного состояния в другое под воздействием внешних сигналов. Переключение триггера из одного состояния в другое происходит значительно быстрее, чем зарядка и разрядка конденсатора в ячейках памяти DRAM [5]. По этой причине SRAM обладает большим быстродействием по сравнению с DRAM и считается самой быстрой памятью на сегодняшний день. Память SRAM способна работать на частоте, достигающей нескольких гигагерц.

Так как триггер сохраняет свое состояние в течение длительного времени без внешнего воздействия, SRAM не требует регенерации памяти и потребляет значительно меньше электроэнергии при своей работе, чем DRAM.

Площадь одной ячейки памяти SRAM определяется формулой $140F^2$ [5], где F — характеристика используемого технологического процесса, которая на сегодня достигает 20 нм. Размер ячейки обуславливается числом транзисторов, из которых она состоит (6—8 транзисторов), а также особенностями соединения полупроводниковых элементов между собой и с линиями связи. По причине большой площади ячейки стоимость 1 мегабайта памяти на основе статической RAM значительно выше стоимости 1 мегабайта памяти на основе динамической. В связи с этим SRAM в основном применяется в качестве регистров и кэш-памяти, где главную роль играет скорость чтения и записи данных, а уже затем объем памяти.

Flash

Другим распространенным видом памяти с произвольным доступом является flash-память. Главным ее отличием от других распространенных RAM является ее энергонезависимость. Ячейка flash-памяти состоит из одного транзистора, как правило, n-ρ-n-типа, с плавающим затвором. Ключевым свойством такого транзистора является сохранение электрического заряда на плавающем затворе [6]. При подаче на управляющий затвор транзистора положительного напряжения он перейдет в открытое состояние. Однако, если в этот момент на плавающем затворе будет находиться избыточный отрицательный заряд, то он компенсирует создаваемое управляющим затвором электрическое поле, препятствуя образованию канала проводимости. В итоге, транзистор остается в закрытом состоянии. Если же на плавающем затворе заряд отсутствует, то канал проводимости будет создан, и транзистор перейдет в открытое состояние. Таким образом, по состоянию транзистора можно определить наличие заряда на плавающем затворе и, как следствие, определить, какой бит информации хранит ячейка памяти. Наличие заряда на плавающем затворе соответствует логической единице, его отсутствие — логическому нулю.

Помещение заряда на плавающий затвор достигается либо методом инжекции горячих электронов, либо методом туннелирования Фаулера — Нордхейма [7]. При применении метода инжекции горячих электронов на сток и управляющий затвор транзистора подается высокое положительное напряжение, позволяющее электронам преодолеть потенциальный барьер, создаваемый слоем диэлектрика, и туннелировать в область плавающего затвора. При чтении информации на затвор и сток транзистора подается меньшее напряжение, при котором эффект туннелирования не наблюдается. Для удаления информации из ячейки на управляющий затвор подается высокое отрицательное напряжение, а на исток — положительное. Это приводит к туннелированию электронов, хранящихся на плавающем затворе, в область истока. Изоляция плавающего затвора не идеальна, в связи с чем срок хранения информации во flash-памяти ограничен и не превышает 10 лет. Следует отметить, что процесс записи и стирания содержимого ячейки flash-памяти приводит к необратимым изменениям в ее структуре, таким как размытие границ ρ-n-переходов, что, в свою очередь, приводит к ограничению числа возможных циклов перезаписей до 100 тысяч раз.

Существует несколько типов строения flash-памяти. Наиболее распространенными являются NOR и NAND [8].

Flash-память типа NOR имеет классическую структуру в виде двумерной матрицы, где на пересечении столбцов и строк устанавливается ячейка памяти. NOR обеспечивает малое время доступа к отдельной ячейке. Flash-память типа NAND представляет собой трехмерный массив. В основе также лежит двумерная матрица, однако вместо одной ячейки памяти на пересечении устанавливается столбец ячеек, соединенных последовательно. Благодаря такой конструкции сильно увеличивается плотность компоновки элементов, но в то же время усложняется алгоритм доступа к ячейкам, что приводит к увеличению времени чтения информации из памяти. Технология NOR, как правило, используется в устройствах для хранения программ микропроцессора, в то время как NAND-технология применяется в устройствах хранения данных, таких как твердотельные и USB-флэш-накопители.

Если сравнивать flash-память с DRAM и SRAM, то к преимуществам следует отнести ее энергонезависимость, высокую плотность размещения элементов и, как следствие, хорошую масштабируемость. Однако в силу физических процессов, лежащих в основе данной технологии, быстродействие flash-памяти ниже, чем у других RAM.

Новые виды RAM

FRAM

Одной из перспективных технологий RAM является сегнетоэлектрическая память произвольного доступа. Данный вид памяти является энергонезависимым, что достигается путем

использования в ячейках памяти сегнетоэлектрика. Сегнетоэлектриком называют материалы, способные в определенном интервале температур к самопроизвольной электрической поляризации [9]. При этом поляризация происходит под воздействием внешнего электрического поля.

Ячейка памяти FRAM имеет структуру, аналогичную ячейке DRAM, и состоит из одного транзистора и одного конденсатора. Но вместо слоя диэлектрика в конденсаторе используется слой сегнетоэлектрика, который может быть поляризован. Принцип работы следующий. На пластины конденсатора подается напряжение, которое создает внутри слоя сегнетоэлектрика электрическое поле. Под действием этого поля часть атомов сегнетоэлектрика, как правило, атомы цинка или титана [10], изменяют свою позицию относительно остальных, что приводит к поляризации вещества. Поляризация, которую имеет сегнетоэлектрик при нулевом значении внешнего электрического поля, называется остаточной поляризацией. Слой сегнетоэлектрика имеет два возможных состояния остаточной поляризации. Одно из них соответствует логической единице, другое — логическому нулю.

Для считывания информации из ячейки FRAM в нее записывается логический нуль. Если на момент записи в ячейке хранился нуль, то ничего не произойдет. Если же в ячейке хранилась логическая единица, то переориентация атомов в слое приведет к появлению на выходе короткого импульса. Наличие этого импульса показывает, что ячейка на момент чтения содержала логическую единицу. Таким образом, процесс чтения информации из ячейки FRAM является деструктивным процессом и требует последующей регенерации данных, что увеличивает энергопотребление FRAM.

Как было сказано выше, сегнетоэлектрики имеют способность к самопроизвольной электрической поляризации только в определенном диапазоне температур. Выход рабочей температуры за пределы данного диапазона приводит к тепловой деполяризации. Другими словами, за пределами рабочего диапазона FRAM не сохраняет информацию. Температура полной деполяризации определенных сегнетоэлектриков достигает 430 градусов Цельсия [11]. Важно отметить, что в устройствах FRAM при температуре в диапазоне от –40 до 85 градусов Цельсия деполяризация незначительна и не приводит к потере данных [11, 12]. Указанный диапазон температур сравним с рабочими диапазонами SRAM и DRAM. Следует также отметить, что сегнетоэлектрики изменяют свою поляризацию в электрических полях и не подвержены влиянию магнитных полей, что обеспечивает защиту хранящейся в памяти информации от деструктивного магнитного воздействия.

MRAM

В последнее время сильное развитие получила технология магниторезистивной памяти, или MRAM (Magnetoresistive Random Access Memory). В отличие от большинства других RAM, принцип действия MRAM основывается не на электрических зарядах или токах, а на магнитных элементах памяти. Магнитный элемент состоит из двух слоев ферромагнетика, разделенных тонким слоем диэлектрика. Намагниченность одного из слоев ферромагнетика постоянна, вектор намагниченности всегда имеет одно и то же направление. Намагниченность другого может изменяться под воздействием внешнего магнитного поля. Ячейка памяти состоит из одного управляющего транзистора и одного магнитного элемента [10].

Процесс хранения и обработки информации в MRAM основывается на эффекте туннельного магнитосопротивления, который заключается в зависимости электрического сопротивления магнитного элемента от взаимной ориентации намагниченности его слоев ферромагнетика. Сопротивление ниже, когда вектора намагниченности сонаправлены, и выше, когда противонаправлены. Считывание информации из ячейки памяти MRAM происходит путем измерения ее сопротивления. Как правило, логической единице соответствует низкое сопротивление ячейки, в то время как логический нуль характеризуется высоким сопротивлением — когда векторы намагниченности противонаправлены.

Запись информации в MRAM первоначально осуществлялась путем перемагничивания переменного слоя ферромагнетика с помощью магнитного поля, создаваемого линиями связи. Такой

способ требовал большой силы тока для создания магнитного поля и, как следствие, большого количества энергии, что делало MRAM не применимым в портативных устройствах, для которых важно малое энергопотребление. Данная проблема была решена с открытием нового способа записи, который основывается на технологии переноса спинового момента (Spin-transfer torque – STT) [13].

Электрические заряды, в том числе и электроны, могут обладать собственным моментом импульса, называемым спином. Электрический ток, в общем случае, является неполяризованным. Если поляризованный электрический ток направить в магнитный слой, то суммарный момент импульса может быть передан этому магнитному слою, изменив ориентацию его магнитного поля. STT позволяет уменьшить значение силы тока, необходимое для записи информации в память MRAM, и, как следствие, снизить уровень энергопотребления при записи информации до уровня энергопотребления при чтении. Так как технология STT стала важнейшим аспектом при использовании MRAM, то сегодня встречаются и другие названия технологии MRAM, например STT RAM или STT-MRAM.

На сегодняшний день MRAM уже обладает скоростью чтения и записи, сравнимой с DRAM, и вскоре может достичь быстродействия SRAM. MRAM обладает плотностью расположения элементов, сравнимой с плотностью компоновки модулей DRAM, и в то же время имеет значительно меньшее энергопотребление и является энергонезависимой памятью. В дополнение она лишена проблемы износа ячеек памяти, которая имеется у технологии флэш. Комбинация всех этих свойств позволяет полагать, что в скором времени память MRAM станет «универсальной памятью» и будет в состоянии заменить другие виды памяти.

PCM

Закончим рассмотрение существующих RAM памятью на основе фазового перехода, или PCM (Phase Change Memory). PCM является новым типом энергонезависимой памяти, принцип действия которого основывается на свойстве халькогенидов быстро переходить из кристаллического состояния в аморфное и наоборот [10]. Кристаллическое и аморфное состояния халькогенидов обладают разными значениями электрического сопротивления. С помощью электрического сопротивления ячейки памяти можно определить, какое значение она хранит: аморфное состояние соответствует высокому сопротивлению и используется для представления логической единицы, кристаллическое состояние соответствует низкому сопротивлению и обозначает логический нуль.

Следует отметить, что переход халькогенидов из кристаллического состояния в аморфное происходит при нагреве до температуры свыше температуры кристаллизации, но ниже температуры плавления.

В ходе изучения различных видов памяти с произвольным доступом было произведено сравнение их числовых характеристик, таких как размер ячейки, быстродействие, количество возможных циклов записей. Результаты представлены в таблице 1. По результатам сравнения можно сделать вывод, что на роль «универсальной» памяти лучше подходят технологии MRAM и PCM, в то время как FRAM имеет ряд ограничений и проблем, которые пока не позволяют ей конкурировать с другими новыми перспективными RAM.

Таблица 1. Сравнение технических характеристик разных видов RAM

	DRAM	SRAM	Flash NOR	Flash NAND	FRAM	MRAM	PCM
Является энергонезависимой	–	–	+	+	+	+	+
Технологический процесс F, нм	20	20	45	17	90	32	20

Площадь ячейки	$4F^2$	$140F^2$	$10F^2$	$4F^2$	$15F^2$	$6F^2$	$4F^2$
Время чтения, нс	10	0,1	10	100	20	10	10
Время записи, нс	10	0,1	10^4	10^3	10	1	50
Срок хранения информации	64 мс	—	10 лет	10 лет	10 лет	20 лет	20 лет
Число возможных перезаписей	1e+16	1e+16	1e+5	1e+5	1e+15	1e+15	1e+9
Напряжение при чтении/записи, В	1,5/1,5	0,7/0,7	10/1,5	15/1,5	1,5/1,5	1/1	1/1

Для анализа возможных уязвимостей СВТ на основе разных типов RAM в статье предлагается разделить уязвимости по аспектам информационной безопасности. Другими словами, предлагается выделить три группы уязвимостей: уязвимости, эксплуатация которых может привести к нарушению конфиденциальности информации, ее целостности или доступности. В то же время среди уязвимостей СВТ можно выделить уязвимости, связанные с окружающей RAM программной и аппаратной средой, и уязвимости, которые основываются на особенностях физических процессов, происходящих в RAM. Первая группа включает уязвимости операционных систем, протоколов обмена данными, прикладного программного обеспечения, запущенного в используемой вычислительной системе, аппаратного обеспечения. Таким образом, уязвимости первой группы зависят от типа используемой памяти и являются актуальными при использовании любой технологии RAM.

Уязвимости второй группы связаны с физическими особенностями процесса хранения информации в разных RAM. В первую очередь следует отметить, что главное различие в методах защиты разных видов RAM основывается на возможности автономного хранения информации без постоянной подачи электроэнергии. Во время работы вычислительной системы в ее оперативной памяти может находиться конфиденциальная информация. Если в качестве оперативной памяти используется энергозависимая память произвольного доступа, то хранящаяся в ней конфиденциальная информация может быть скомпрометирована только при сохранении подачи на нее электроэнергии. При отключении энергии хранящаяся информация со временем будет потеряна. Однако следует сказать, что информация, хранящаяся в энергозависимой RAM, может быть скомпрометирована путем реализации атаки холодной перезагрузки (cold boot attacks). Данный вид атак основывается на том, что при выключении компьютера без использования средств операционной системы, например отключением питания компьютера, информация, хранящаяся в оперативной памяти, не очищается. Если при этом охладить модуль оперативной памяти, то время хранения информации без подачи электроэнергии будет увеличено. В частности, при охлаждении модуля памяти до экстремально низких возможных рабочих температур, таких как –50 градусов Цельсия, информация в микросхеме может сохраняться в течение нескольких часов и даже дней [14]. Для энергонезависимых типов RAM данная атака еще более актуальна, так как информация будет храниться в модуле памяти почти неограниченное количество времени (несколько лет) при сохранении рабочего диапазона температур и отсутствии внешних деструктивных электромагнитных воздействий. Процесс защиты от атак холодной перезагрузки имеет две составляющие. Первая представляет собой ограничение физического доступа к СВТ. Этого можно добиться путем ввода на объекте контролируемой зоны, разграничения зон доступа сотрудников, присвоения сотрудникам личных идентификационных ключей. Вторая составляющая — обязательная очистка памяти или определенных ее областей при аварийном отключении питания. При корректном завершении

работы вычислительной системы очисткой RAM занимается операционная система. При аварийном завершении очистки памяти не происходит, и в ней может остаться конфиденциальная информация. Предлагается использовать дополнительный аппаратный модуль с автономным источником питания, который при наступлении определенных условий (отключение питания, вскрытие корпуса) удалял бы все хранящиеся в RAM данные или очищал определенные ее области.

Следует также отметить, что для некоторых видом RAM возможно восстановление данных даже после их удаления из памяти. В частности, в MRAM существует возможность восстановления информации по взаимной ориентации векторов намагниченности слоев ферромагнетиков. Для исключения такой возможности необходимо многократное стирание содержимого ячейки. Такую функцию возможно реализовать на базе того же дополнительного аппаратного модуля.

В качестве уязвимостей, эксплуатация которых может привести к нарушению конфиденциальности информации, следует учитывать и побочные электромагнитные излучения и наводки (ПЭМИН). В данной статье не приводится каких-либо конкретных цифр уровня ПЭМИН рассмотренных видов RAM. Анализ и рассмотрение влияния ПЭМИН на описанные выше типы памяти выходят за рамки данной статьи, так как требуют дополнительных исследований.

Угрозы нарушения целостности и доступности информации, как правило, связаны с различными внешними деструктивными воздействиями. Они могут заключаться в изменении температуры, электромагнитном воздействии, отключении питания системы для энергозависимых RAM. Диапазоны рабочих температур для разных видов RAM представлены в таблице 2.

Таблица 2. Сравнение диапазона рабочих температур различных типов RAM

Тип RAM	DRAM	SRAM	Flash	FRAM	MRAM	PCM
Диапазон температур, °C	-40 – +110	-40 – +100	-40 – +90	-40 – +85	-40 –+125	0 – +70

Приведенный список внешних воздействий не является полным. Для составления полного списка возможных деструктивных воздействий необходимы дополнительные детальные исследования каждого вида памяти, которые на данном этапе работы не проводились.

Таким образом, на основании исследований, которым посвящена данная статья, можно сделать вывод, что оптимальными видами памяти, которые были бы энергонезависимыми, сочетали в себе высокое быстродействие, малое энергопотребление, высокую плотность расположения элементов, являются MRAM и PCM. Переход на эти типы RAM в СВТ не приведет к появлению новых уязвимостей, так как источником большинства уязвимостей является окружающая программно-аппаратная среда. Эксплуатация уязвимостей, связанных с переходом на энергонезависимые RAM, может быть заблокирована путем применения методов защиты, упоминаемых в статье. Следует отметить, что наличие энергонезависимой RAM, обладающей достаточным быстродействием и плотностью элементов, позволяет задуматься о создании нового типа архитектуры компьютера с единым физическим адресным пространством. Переход вычислительных систем на архитектуру с единым адресным пространством позволит значительно увеличить быстродействие систем, снизит их энергопотребление. Однако такой переход будет требовать совершенно новых способов организации вычислительных систем и, как следствие, механизмов их защиты. Дальнейшие исследования по возможности создания безопасной архитектуры с единым адресным пространством будут освещены в последующих работах.

СПИСОК ЛИТЕРАТУРЫ:

1. *Степаненко О. С.* Настройка персонального компьютера. Установки BIOS. Самоучитель. 2-е издание: М.: ООО «И. Д. Вильямс», 2007 — 480с.
2. *Kaspersky K.* Code Optimization: Effective Memory Usage. LIST Publishing. 2003 — 389с.
3. *Keeth B., Baker R. J.* DRAM Circuit Design: A Tutorial. John Wiley & Sons. 2001 — 200с.
4. Hynix semiconductor Inc. The future memory technology. Sung-ki Park, October 27. 2011. [Электронный ресурс]: Symantec. URL: http://www.sematech.org/meetings/archives/symposia/10202/Keynote-Intro/Park_The%20future%20memory%20technologies.pdf (дата обращения: 23.04.2014).
5. Advanced Digital Integrated Circuits. Lecture 9-12: SRAM Design // EE241. Spring 2013. [Электронный ресурс]: Berkeley. URL: http://bwrcs.eecs.berkeley.edu/Classes/icdesign/ee241_s13/Lectures/Lecture9-SRAM-annotated.pdf (дата обращения: 23.04.2014).
6. Macronix International Co. Introduction to NAND in Embedded Systems // REV. 2. February 20. 2014. [Электронный ресурс]: Macronix International Co. URL: http://www.macronix.com/Lists/ApplicationNote/Attachments/736/AN0269V2_Introduction%20to%20NAND%20in%20Embedded%20Systems-0220.pdf
7. *Пахомов С.* Флэш-память на любой вкус // КомпьютерПресс. 2004. Ноябрь. [Электронный ресурс]: КомпьютерПресс. URL: http://compress.ru/article.aspx?id=12401 (дата обращения: 23.04.2014).
8. *Kwon W., King Liu T. J., Subramanian V.* Novel Technologies for Next Generation Memory // Electrical Engineering and Computer Sciences University of California at Berkeley. July 25. 2013.
9. *Щербаченко Л., Каранков В., Марчук С.* Исследование поляризации сегнетоэлектриков // ГОУ ВПО ИГУ. Кафедра общей физики. 2005. [Электронный ресурс]: Российское образование, федеральный портал. URL: http://window.edu.ru/resource/168/30168/files/isu046.pdf (дата обращения: 23.04.2014).
10. *Muneed M., Akhram I., Nazir A.* Non-volatile Random Access Memory Technology (MRAM, FeRAM, PRAM) // Smart Electronic Materials.
11. *Thanigai P.* FRAM Quality and Reliability // SLAA526. March 2012. [Электронный ресурс]: TehasInstruments. URL: http://www.ti.com/lit/an/slaa526/slaa526.pdf (дата обращения: 23.04.2014).
12. *Bohac C.* Comparing Technologies: MRAM vs. FRAM // Application Note 02130. March 2013. [Электронный ресурс]: Everspin Technology. URL: http://www.everspin.com/PDF/EST02130_Comparing_Technologies_FRAM_vs_MRAM_AppNote.pdf (дата обращения: 23.04.2014).
13. *Apalkov D., Khvalkovskiy A., Watts S., Nikitin V., Tang X., Lottis D., Moon K., Luo X., Chen E., Ong A., Driskill-Smith A., Krounbi M.* Spin-Transfer Torque Magnetic Random Access Memory (STT-MRAM) // ACM Journal on Emerging Technologies in Computing Systems (JETC). 2013. May 7. Vol. 9 (2).
14. *Halderman J. A., Schoen S. D., Heninger N., Clarkson W., Paul W., Calandrino J. A., Feldman A. J., Appelbaum J., Felten E. W.* Lest We Remember: Cold Boot Attacks on Encryption Keys // USENIX Security Symposium. July 2008. [Электронный ресурс]: Amazon. URL: http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/coldboot.pdf (дата обращения: 23.04.2014).

REFERENCES:

1. *Stepanenko O. S.* Nastroiyka personalnogo komputera. Ustanovki BIOS. Samouchitel, 2-e izdanie. M. OOO "I.D. Viliayms", 2007.
2. *Kaspersky K.* Code Optimization: Effective Memory Usage — LIST Publishing, 2003.
3. *Keeth B., Baker R. J.* DRAM Circuit Design: A Tutorial — John Wiley & Sons, 2001.
4. Hynix semiconductor Inc. The future memory technology — Sung-ki Park, October 27, 2011. Symantec. URL: http://www.sematech.org/meetings/archives/symposia/10202/Keynote-Intro/Park_The%20future %20memory%20technologies.pdf. 23.04.2014.
5. Advanced Digital Integrated Circuits. Lecture 9-12: SRAM Design — EE241, Spring 2013. Berkeley. URL: http://bwrcs.eecs.berkeley.edu/Classes/icdesign/ee241_s13/Lectures/Lecture9-SRAM-annotated.pdf. Data obrasheniya: 23.04.2014.
6. Macronix Internatinal Co. Introduction to NAND in Embedded Systems — REV. 2, February 20, 2014.
7. *Pakhomov S.* Flesh-pamayt na luboiy vkus — KomputerPress, Noaybr, 2004, [Elektronniy resurs]: KomputerPress. URL: http://compress.ru/article.aspx?id=12401. Data obrasheniya: 23.04.2014.
8. *Kwon W., King Liu T. J., Subramanian V.* Novel Technologies for Next Generation Memory — Electrical Engineering and Computer Sciences University of California at Berkeley, July 25, 2013.
9. *Sherbachenko L., Karankov V., Marchuk S.* Issledovanie polayrizatsii segnetoelektrikov —GOU VPO IGU, Kafedra fiziki, 2005.
10. *Muneed. M., Akhram I., Nazir A.* Non-volatile Random Access Memory Technlogy (MRAM, FeRAM, PRAM) — Snart Electronic Materials
11. *Thanigai P.* FRAM Quality and Reliability — SLAA526, March 2012. TehasInstruments. URL: http://www.ti.com/lit/an/slaa526/slaa526.pdf. 23.04.2014.
12. *Bohac C.* Comparing Technologies: MRAM vs. FRAM — Application Note 02130, March 2013. [Электронный ресурс]: Everspin Technology. URL: http://www.everspin.com/PDF/EST02130_Comparing_Technologies_FRAM_vs_MRAM_AppNote.pdf. 23.04.2014.
13. *Apalkov D., Khvalkovskiy A., Watts S., Nikitin V., Tang X., Lottis D., Moon K., Luo X., Chen E., Ong A., Driskill-Smith A., Krounbi M.* Spin-Transfer Torque Magnetic Random Access Memory (STT-MRAM) — ACM Journal on Emerging Technologies in Computing Systems (JETC), Volumes 9(2), May 7, 0213.
14. *Halderman J. A., Schoen S. D., Heninger N., Clarkson W., Paul W., Calandrino J. A., Feldman A. J., Appelbaum J., Felten E. W.* Lest We Remember: Cold Boot Attacks on Encryption Keys — USENIX Security Symposium, July 2008.