ОПРЕДЕЛЕНИЕ СПОСОБА РАЗРУШЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ПЕРИОДОМ АКТУАЛЬНОСТИ НА МОБИЛЬНЫХ УСТРОЙСТВАХ ХРАНЕНИЯ ДАННЫХ

А. М. Шалыгин, А. А. Ершов, Д. Б. Николаев, К. С. Шилкин, А. И. Юрищев

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

В современном мире, нацеленном на дальнейшее развитие электронных систем информационного взаимодействия и электронного документооборота, роль, которую играют мобильные устройства хранения данных на основе встроенных микроконтроллеров и микросхем памяти различного объема, продолжает увеличиваться.

Вместе с этим возрастает и важность информации, которую мы доверяем данным устройствам: от персональных данных до информации правительственной важности. В этой ситуации потеря или кража мобильного устройства с конфиденциальной информацией может обернуться утратой, как минимум, деловой репутации.

Для мобильных устройств с информацией определенного уровня важности на этапе транспортировки существует явная угроза их захвата нарушителем, а, следовательно, для подобных устройств необходимо обеспечить сохранение конфиденциальности хранящейся на них информации.

Наиболее очевидный и применяемый веками способ сохранения конфиденциальности информации – преобразование данных. Достигшее за это время значительного развития и обеспечивающее достаточно высокий уровень защиты информации преобразование данных в ряде случаев не может обеспечить своей криптостойкости, в силу обстоятельств, связанных с особенностями эксплуатации мобильного устройства и необходимостью распределения параметров преобразования между владельцами и получателями конфиденциальной информации. Данное утверждение поясняется следующими положениями условий эксплуатации. Для осуществления прямого и обратного преобразования информации необходимым является наличие параметров преобразования, как у владельца информации, так и у получателя. Таким образом, необходимо наличие закрытого канала связи между ними, что в ряде случаев является невозможным. Передача же параметров преобразования лицу (курьеру), осуществляющему транспортировку информации на мобильном устройстве, рассматривается как мера, компрометирующая применение преобразования данных в условиях применения к курьеру мер физического воздействия со стороны нарушителя.

Таким образом, в ситуациях, когда криптоалгоритмы не могут быть применены для обеспечения безопасности информации на мобильном устройстве хранения данных или обеспечиваемая криптостойкость информации считается недостаточной, является очевидным построение защиты на принципе недопущения захвата информации «любыми средствами», включая средства разрушения информации вплоть до разрушения самого мобильного устройства хранения данных при попытке захвата. Отметим, что средства разрушения информации не замещают преобразование данных, а являются дополнительным к преобразованию повышением уровня защищенности информации.

Целью данной работы является определение метода разрушения информации с ограниченным периодом актуальности на мобильных устройствах хранения данных. Достижение цели обеспечивается решением следующих задач:

− определение требуемой степени разрушения информации;

− разработка критериев применимости различных методов разрушения информации;

− анализ различных методов разрушения информации.

Поскольку многообразие методов разрушения информации велико и эффективность их применения различна, то перед рассмотрением различных методов целесообразно выполнить анализ требуемой степени разрушения информации и степени разрушения ее носителя (устройства хранения или его узлов).

При решении задачи разрушения информации принципиальным является рассмотреть следующие два взаимосвязанных понятия:

− период актуальности захватываемой информации;

− средства восстановления информации, которыми располагает нарушитель.

Под периодом актуальности информации следует предполагать период времени с момента захвата нарушителем устройства хранения данных до момента, когда обладание им потеряет для него привлекательность. Длительность периода актуальности информации напрямую зависит от характера применения защищаемой информации и фактически определяет время, которым располагает нарушитель для достижения своих целей.

Под средствами восстановления информации подразумеваются технические средства, при помощи которых нарушитель пытается восстановить разрушенную информацию. Эффективность восстановления напрямую зависит от осведомленности нарушителя в устройстве хранения и разрушения информации, а также от времени, которым он располагает для достижения своих целей.

1. Анализ требуемой степени разрушения информации и разработка критериев выбора метода разрушения информации

Многообразие возможных методов и путей разрушения информации ограничено только творческими способностями исследователя и современными достижениями технических наук. Применимость различных методов ограничивается типом устройства хранения данных, его конструктивными и эксплуатационными особенностями. Рассматриваемое в данной работе носимое устройство хранения данных построено на микросхеме электронно-перепрограммируемой постоянной памяти, имеет внутренние аппаратное обеспечение и программный алгоритм чтения и перезаписи информации. Аппаратное обеспечение и программный алгоритм чтения и перезаписи информации реализованы в управляющем модуле устройства хранения (рис. 1), построенном на микроконтроллере со встроенной или внешней памятью программ. Причем, в частном случае память, используемая для хранения информации, и память программы управления (алгоритма чтения и перезаписи) работой устройства могут быть выполнены в одной микросхеме – микроконтроллере с электрически перепрограммируемой памятью.

Кроме управляющего модуля и микросхемы хранения информации в состав устройства хранения данных входит интерфейс взаимодействия с внешними устройствами и обеспечения электропитания от внешних источников.

В принципе представленная структура типична для большинства устройств хранения данных, как для узкоспециализированных устройств (электронные ключи, пропуска и т. д.), так и для устройств – накопителей информации, построенных на основе микросхем памяти.

Для рассматриваемого типа устройств хранения данных разрушение информации может быть реализовано двумя принципиально различными путями (рис. 2):

− разрушение устройства хранения данных или его отдельных узлов;

− перезапись электронной памяти устройства хранения данных, исключающая разрушение его узлов.

Представленные варианты различны, в первую очередь, физическими принципами, лежащими в основе разрушающего воздействия и разграничивающими методы разрушения информации.

Разрушающее воздействие может быть направлено как на устройство хранения данных в целом, так и на его отдельные узлы. Выбор объекта воздействия (внутриплатные соединения, микросхемы памяти и др.) влияет на время восстановления информации и необходимый для этого арсенал средств восстановления.

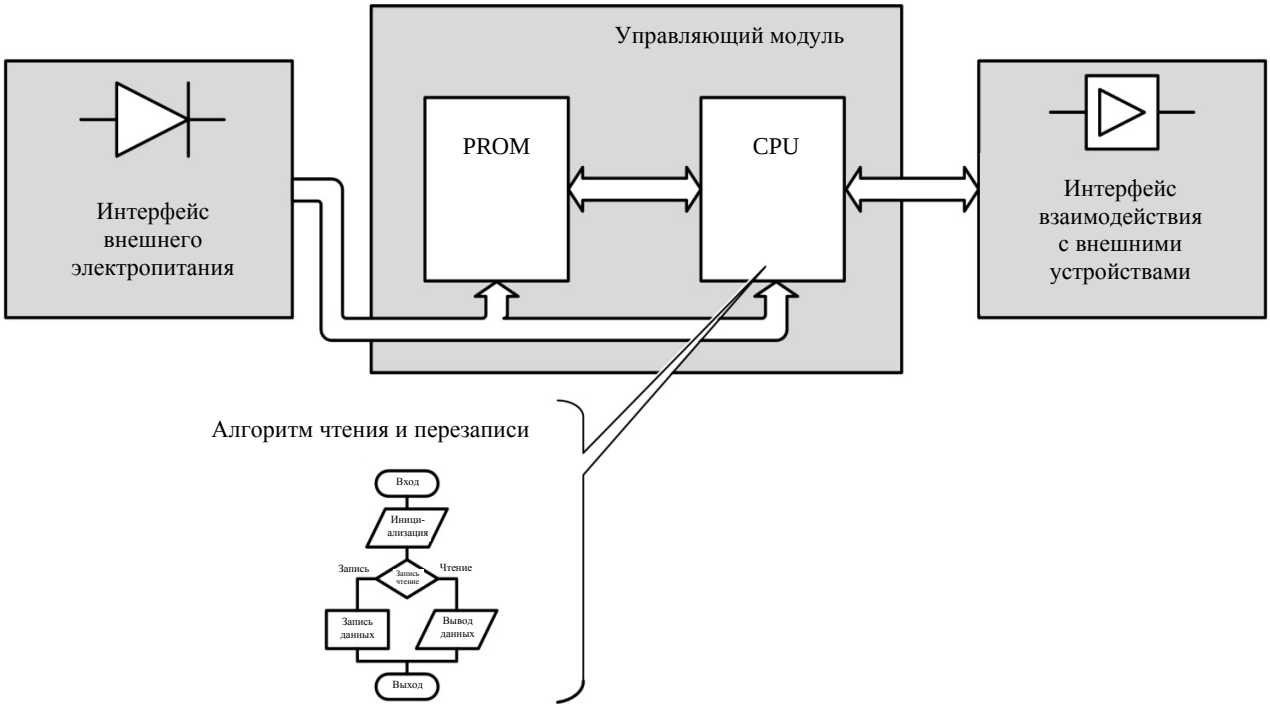

Рис. 1. Структура устройства хранения данных

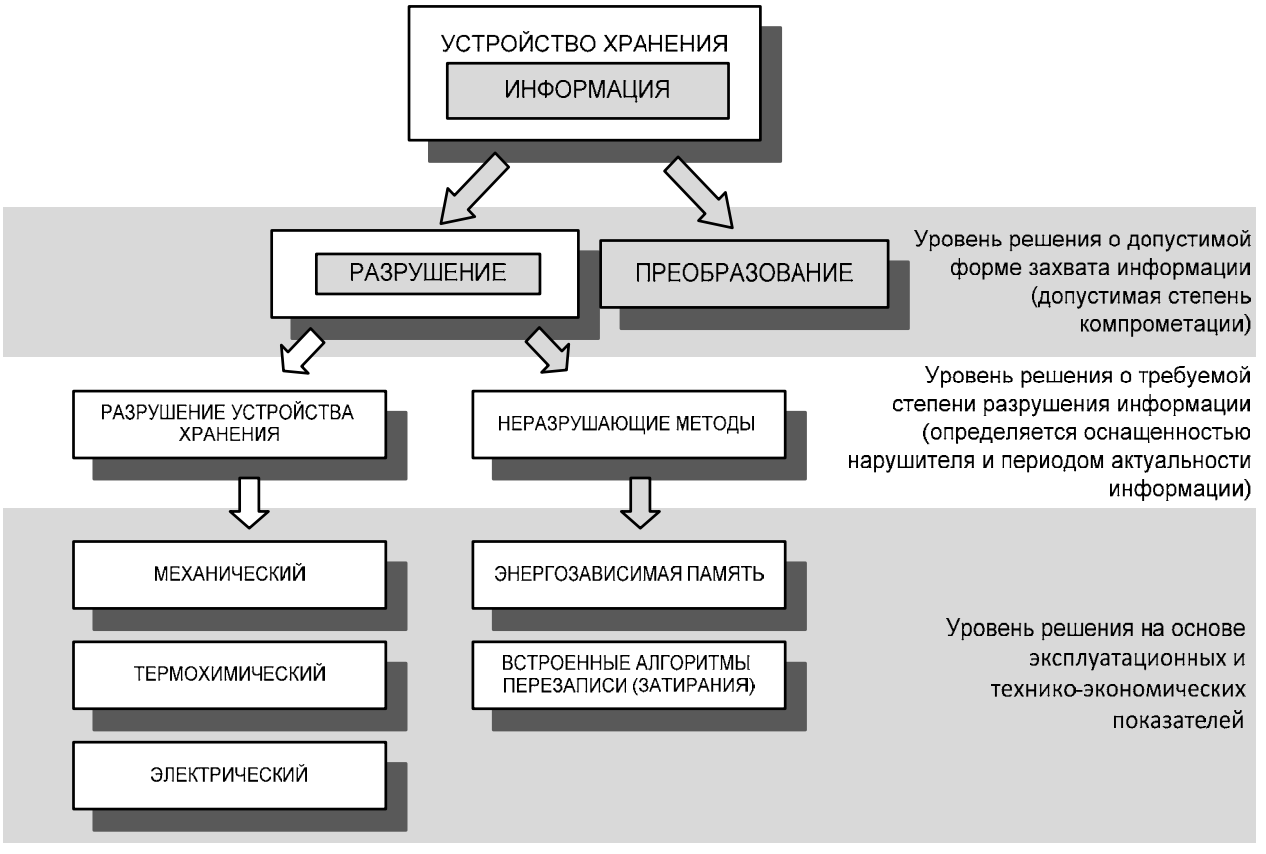

Рис. 2. Условное представление направлений исследований

Выбор пути разрушения информации может быть осуществлен на основании оценки характеристик модели нарушителя, а именно, времени, которым располагает нарушитель для достижения своих целей и его технической оснащенности. В литературе [2], посвященной вопросу разрушения информации, бесспорным является утверждение о том, что гарантированное разрушение возможно только при разрушении непосредственного носителя информации, т. е. максимально возможная степень разрушения информации достигается разрушающими устройство хранения данных методами. Однако, в случае, когда нарушитель в своих действиях ограничен жесткими временными рамками (периодом актуальности информации), а, следовательно, испытывает стеснение в применении средств восстановления информации (при этом не испытывая недостатка в осведомленности конструкции), мы можем говорить о снижении степени разрушения информации.

Таким образом, в ситуации ограниченности нарушителя жесткими временными рамками целесообразно ориентироваться при выборе метода разрушения информации на совокупность факторов, связанных с качественными эксплуатационными и технико-экономическими характеристиками мобильного устройства хранения данных, непосредственное влияние на которое оказывает конструкция устройства разрушения информации.

На основании вышесказанного стратегия поиска метода разрушения может быть сформулирована следующим образом: разрабатываемый метод должен обладать, в первую очередь, не максимальной эффективностью разрушения информации, а обеспечивать оптимальное сочетание качественных эксплуатационных и технико-экономических показателей устройства хранения и разрушения информации, таких как:

− минимальное время разрушения информации;

− ремонтопригодность устройства после проведения разрушения информации;

− эксплуатационная безопасность;

− массогабаритные характеристики;

− стоимость изготовления и эксплуатации.

Приведенные показатели являются критериями поиска метода разрушения информации, при этом следует учитывать, что выбранный метод разрушения информации должен обеспечивать степень разрушения, для которой время восстановления информации максимально эффективным методом на порядок больше, чем период актуальности информации.

2. Анализ методов разрушения информации и механизмов на их основе

2.1. Обзор методов разрушения информации

Общий обзор перспективных, с точки зрения авторов, методов разрушения устройств хранения данных или его отдельных узлов позволяет выделить их

в три группы в соответствии с типом разрушающего воздействия (рис. 2):

− методы механического разрушения;
− методы термохимического разрушения;
− методы электрического разрушения.

Особое внимание в работе уделено неразрушающим устройство хранения данных методам разрушения информации, основанным на перезаписи электронной памяти.

В основе методов механического разрушения лежит механический характер разрушающего воздействия на узлы устройства хранения данных, при этом в качестве источника воздействия могут быть как физическое усилие человека или пружины, так и энергия подрыва пиропатрона. В частности, разрушение микросхемы памяти может быть реализовано направленным на нее усилием пробойника.

В основе термохимического разрушения лежит явление самораспространяющегося высокотемпературного синтеза (СВС). Составы СВС способны обеспечить локальный разогрев устройства хранения данных до температуры в 3000 K и выше без использования специальных печей.

В основе методов электрического разрушения лежит свойство деградации полупроводниковых структур при тепловом воздействии протекающего тока. С данным свойством полупроводников связано значение зависимости импульсной электрической прочности от длительности одиночного импульса напряжения. Воздействующим фактором при электрическом разрушении является импульс или пачка импульсов напряжения, подаваемая выборочно или на совокупность выводов микросхемы.

Непосредственными носителями информации являются полупроводниковые структуры (вентили), различие в состоянии которых определяет наличие или отсутствие информации и ее содержание. Вследствие этого помимо разрушения узлов электронного носителя следует рассмотреть разрушение информации путем перезаписи полупроводниковых структур при сохранении их работоспособного состояния. Применение неразрушающих устройство хранения методов в ситуациях, когда нарушитель ограничен периодом актуальности информации, рассматривается авторами как значительно более перспективное (по сравнению с разрушающими методами).

2.2. Время разрушения информации

Как говорилось выше, механизм разрушения активируется курьером, осуществляющим транспортировку устройства хранения информации, в ситуации возникновения угрозы захвата мобильного устройства. Подразумевается, что на момент захвата механизм разрушения информации уже запущен, при этом нарушитель может попытаться остановить процесс разрушения информации. Приведенные выше разрушающие методы имеют приблизительно равное, относительно малое время разрушения информации (менее 1 с). Для устройства хранения данных на базе низкопроизводительного процессора со встроенной Flash ПЗУ емкостью 2 Кбайт наибольшее время для разрушения записанной в нем информации – порядка 2,5 с – требуется при использовании неразрушающих устройство хранения данных методов разрушения информации. Аналогичная ситуация (наибольшее время требует неразрушающий устройство хранения метод) будет наблюдаться при применении более высокопроизводительных микроконтроллеров и микросхем памяти большего объема. Таким образом, при обеспечении соответствующей конструктивной защиты (против действий нарушителя) процессы разрушения информации фактически невозможно остановить вследствие их высокой скоротечности.

2.3. Ремонтопригодность устройства

Очевидно, что применение разрушающего воздействия как к устройству хранения данных в целом, так и к его отдельным узлам влечет за собой необходимость ремонта разрушенных элементов перед дальнейшей эксплуатацией устройства хранения. Так как общим для всех методов является возможность сконцентрировать разрушение на отдельных элементах [1], то теоретически мероприятия по ремонту устройства хранения заключаются в замене разрушаемых элементов. Однако конечная степень разрушения всех элементов устройства зависит от конструкции механизма разрушения, степени ее проработки и точности ее реализации. В связи с этим мероприятия по ремонту устройства хранения должны содержать осмотр всех элементов устройства на предмет разрушения, замену поврежденных элементов и проверку работоспособности устройства в целом. В конечном счете, для определения объема ремонтных мероприятий необходима экспериментальная отработка устройств хранения данных, реализующих разрушение информации.

Преимуществом неразрушающих устройство хранения данных методов разрушения информации является отсутствие необходимости в проведении ремонтных мероприятий после разрушения информации, так как устройство хранения данных полностью сохраняет свою работоспособность. Данный фактор значительно удешевляет эксплуатацию устройства хранения данных и делает процесс эксплуатации независимым от изготовителя устройства.

2.4. Эксплуатационная безопасность

Сомнение в эксплуатационной безопасности могут вызывать такие методы разрушения устройств хранения данных, как термохимические и механические, в которых применяются в качестве источников воздействия составы СВС и пиропатроны соответственно.

Здесь важно отметить факторы, которые обеспечивают высокий уровень эксплуатационной безо-

пасности термохимических методов. Температура воспламенения значительной части составов СВС лежит в диапазоне от 600 до 1200 °С, что исключает самовоспламенение при установке их на работающие элементы электронной аппаратуры, а горение большинства составов СВС ни при каких условиях не переходит в детонацию.

В настоящее время применение пиропатронов и устройств на их основе получило широкое распространение в различных областях человеческой деятельности: ракетостроение, автомобилестроение, охранные системы, спасательная техника, парашютный спорт и т. д. Многолетняя практика гражданского применения пиропатронов в различных, в т. ч. и электронных, устройствах показала их эксплуатационную безопасность.

2.5. Массогабаритные характеристики

Наименьшими массогабаритными характеристиками обладает механизм неразрушающего устройство хранения данных метода разрушения информации. Данный факт объясняется тем, что для реализации этого метода требуется незначительная схемотехническая доработка устройства хранения и его программного обеспечения. Основным же фактором, определяющим увеличение массогабаритных характеристик устройства хранения данных при установке в него механизма разрушения информации, является внутренний источник электропитания относительно малой емкости, например, ионистор К58-6а-5,5В-0,68Ф (с диаметром 21 мм, высотой 9 мм и массой 11,6 г).

Незначительно большими массогабаритными характеристиками обладает механизм термохимического метода разрушения информации, что объясняется наличием брикета из состава СВС с массой в несколько граммов и размерами микросхемы памяти, а также внутреннего источника электропитания, например, ионистора К58-4-2,5В-4,7Ф (с диаметром 24,5 мм, высотой 2,5 мм и массой 5 г), обеспечивающего импульсный ток не менее 0,4 А для задействования электровоспламенителя.

Реализация механизма электронного разрушения информации подразумевает схемотехническую доработку устройства хранения данных, которая включает в себя, кроме установки внутреннего источника электропитания, применение схемы генерации высоковольтных импульсов (порядка 8−10 кВ), состоящей из двух относительно больших по размеру трансформаторов, емкостей и еще порядка десятка радиоэлементов. Габаритные размеры монтажной платы с размещенными на ней схемой генерации импульсов и внутренним источником электропитания составляют приблизительно 100×50×10 мм.

Наихудшие массогабаритные характеристики, а также эргономические показатели имеет устройство хранения данных, реализующее механический метод разрушения информации. Это объясняется двумя факторами, определяющими конструкцию всего устройства: принципом механического разрушения и сложностью исполнения механизма разрушения. Дело в том, что пробойник должен быть размещен в плоскости, ортогональной к плоскости разрушаемой микросхемы, что влечет за собой необходимость расположения микросхем и других электронных компонентов на отдельных печатных платах, скомпонованных по принципу этажерки. Второй фактор объясняется тем, что, несмотря на относительно небольшие размеры пружин механизма разрушения (диаметром от 9 до 13 мм и высотой во взведенном состоянии около 6 мм), значительное механическое усилие, обеспечиваемое ими (не менее 125 Н), требует разработки сложного механизма их удержания и спуска (приведения в действие пробойника). Таким образом, устройство хранения и разрушения информации может иметь вид цилиндра с диаметром основания 30−40 мм и высотой от 70 до 100 мм.

2.6. Стоимость изготовления и эксплуатации

Стоимость разработки и изготовления образца устройства хранения и разрушения информации определяется количеством различных компонентов, входящих в состав конструкции устройства, сложностью их изготовления и количеством привлекаемых для этого соисполнителей. В связи с этим наиболее дорогостоящими представляются устройства, реализующие термохимический и механический на основе пиропатронов методы разрушения информации, так как требуют для разработки и изготовления привлечения специалистов соответствующих областей.

Стоимость эксплуатации определяется необходимостью технического обслуживания устройства хранения и разрушения информации. Очевидно, что периодические проверки работоспособности механизма разрушения информации могут проводиться только в устройствах, реализующих неразрушающий устройство хранения метод разрушения информации. Регламент технического обслуживания должен предусматривать проверку работоспособности и замену в случае неисправности внутреннего источника электропитания.

При построении устройств хранения и разрушения информации на основе электрического разрушения техническое обслуживание может быть выполнено проверкой и заменой (при необходимости) внутреннего источника электропитания. Поскольку остальные элементы (электрорадиоизделия) механизма разрушения слабо подвержены процессам старения, то можно считать (при соответствующем подборе радиоэлементной базы) данный объем обслуживания достаточным для подтверждения надежности всего механизма разрушения в пределах гарантированных сроков службы радиоэлементов.

Техническое обслуживание устройств, реализующих термохимический и механический методы разрушения информации, может быть выполнено

проверкой и заменой (при необходимости) внутреннего источника электропитания, а также заменой отдельных узлов механизмов разрушения, таких как брикеты составов СВС, пружины и пиропатроны. Последнее обстоятельство требует (в отличие от приведенных выше методов разрушения информации) привлечения к техническому обслуживанию предприятий-изготовителей, что ведет к значительному удорожанию эксплуатации подобных устройств. Однако необходимость в данных мероприятиях может отпасть при дальнейшей более тщательной проработке конструкции и подборе узлов механизма разрушения. Данное положение основано на следующем:

− применение в качестве внутренних источников электропитания конденсаторов с двойным электрическим слоем (ионисторов) значительно увеличивает сроки службы источников (до 20 лет);

− составы СВС обладают, как правило, значительной химической устойчивостью, что позволяет встраивать их в аппаратуру на весь срок ее эксплуатации без периодических замен [1];

− пружины в статическом (взведенном) состоянии могут сохранять свои параметры в течение длительного времени (десятки лет).

3. Неразрушающий устройство хранения механизм разрушения информации

Из приведенного анализа различных механизмов разрушения информации видны следующие преимущества неразрушающего устройство хранения механизма разрушения информации:

− полное сохранение работоспособности устройства хранения и разрушения информации после проведения разрушения;

− минимальное количество элементов и простота конструкции механизма разрушения информации;

− возможность полной проверки работоспособности механизма разрушения информации в ходе технического обслуживания;

− независимость пользователя устройства хранения и разрушения информации от производителя устройства;

− наименьшее количество соисполнителей, привлекаемых для разработки и изготовления устройства хранения и разрушения информации.

Таким образом, из вышесказанного следует, что применение метода перезаписи электронной памяти для разрушения информации с ограниченным периодом актуальности в мобильных устройствах хранения данных является более перспективным, с точки зрения эксплуатационных и технико-экономических показателей.

Также отметим, что восстановление разрушенной информации после применения рассматриваемого метода, также как при применении разрушающих методов, невозможно без специальной аппаратуры и микроэлектронного исследования кристалла микросхемы памяти.

Устройство хранения и разрушения информации путем изменения состояния полупроводниковых структур (рис. 3) может быть построено на основе описанной выше конструкции устройства хранения данных путем доработки в части:

− разработки и интегрирования в алгоритм работы устройства хранения программного модуля, реализующего программную перезапись требуемой области памяти по команде «разрушение информации» от аппаратных средств;

− разработки аппаратной части механизма разрушения информации и его схемотехнической интеграции в устройство хранения, включая расчет параметров внутреннего источника электропитания;

− изменения конструктивного исполнения электронного носителя в части размещения внутреннего источника электропитания и аппаратной части механизма разрушения информации.

Программный модуль, обеспечивающий программную перезапись требуемой области памяти, имеет довольно простой алгоритм работы, не вносит значительных издержек в размер основной программы устройства хранения данных и включает в себя процедуры:

− перехвата управления от основной программы алгоритма работы электронного носителя при включении электропитания и проверки наличия команды «разрушение информации» от аппаратной части механизма разрушения;

− циклической перезаписи требуемой области памяти при наличии команды «разрушение информации».

Аппаратная часть механизма разрушения информации построена на переключателе SB с двумя контактными группами, обеспечивающем:

− формирование команды «разрушение информации» ($U_{упр}$) для управляющего модуля (исполняющего программный алгоритм) – первая контактная группа;

− подключение электропитания от внутреннего источника (U_{cc}) к управляющему модулю и микросхеме памяти – вторая контактная группа.

Потери емкости внутреннего источника, вызванные токами утечки (саморазрядом источника тока), напрямую зависят от типа источника тока и могут варьироваться в достаточно широких пределах (1–30 % в месяц). Значение необходимой электрической емкости источника энергии на несколько порядков меньше, чем номиналы емкостей источников тока, выпускаемых промышленностью, а соответственно, несоизмеримо с величиной саморазряда. Таким образом, значение емкости источника тока необходимо выбирать из условия недопущения саморазряда за время между циклами зарядки или периода замены незаряжаемого источника электропитания.

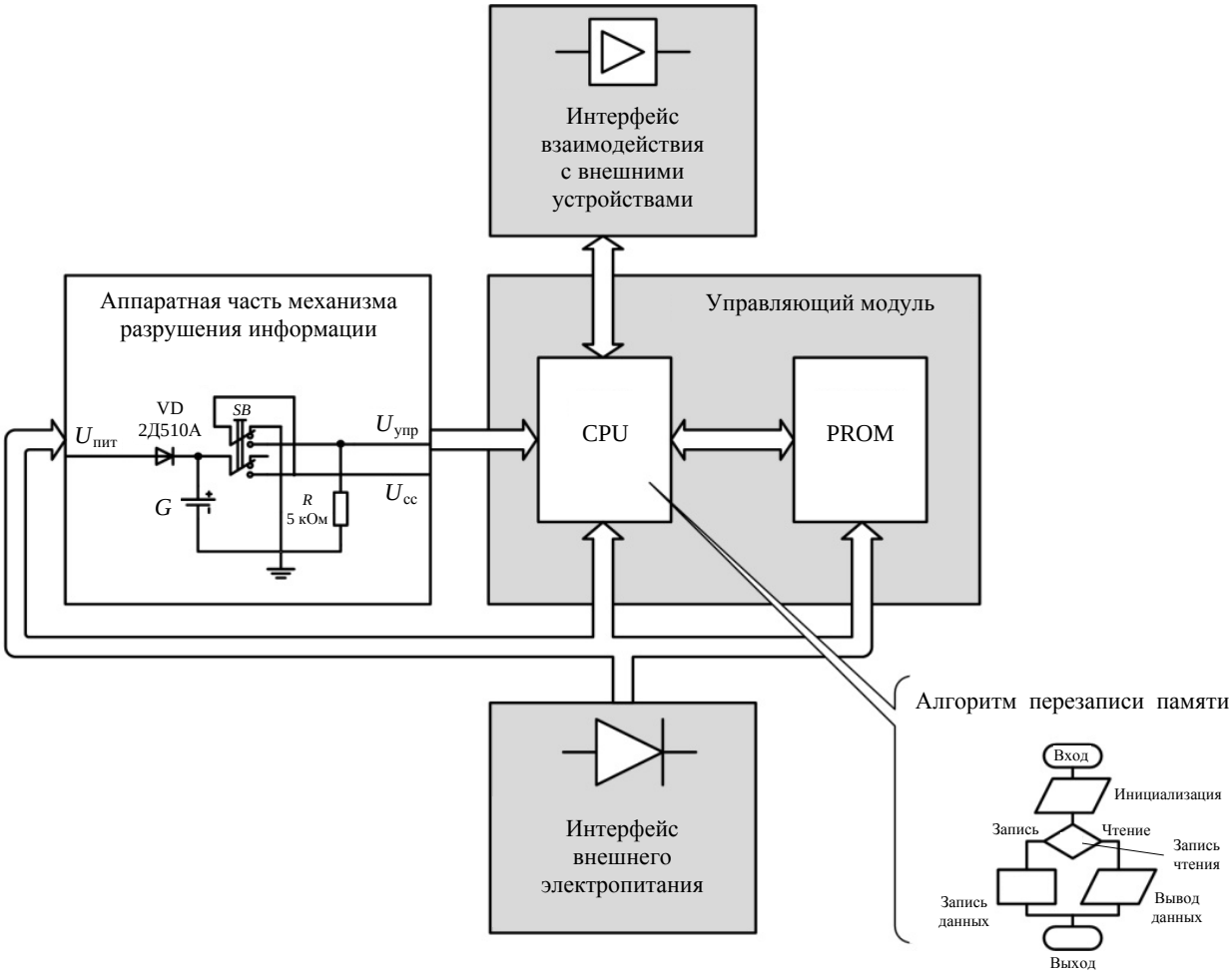

Рис. 3. Структура устройства хранения и разрушения информации

Заключение

В данной статье изложены результаты теоретических исследований модели применения механизмов разрушения информации с ограниченным периодом актуальности в мобильных устройствах хранения данных. Результатом является формулировка:

− концепции построения механизмов разрушения информации с ограниченным периодом актуальности, ориентированной не на достижение максимальной степени разрушения информации, а на достижение наилучших эксплуатационных и технико-экономических характеристик мобильного устройства;

− критериев анализа механизмов разрушения информации, разработанных на основе различных методов разрушения информации.

Выполненные разработка и анализ различных механизмов разрушения информации позволили расчетно-экспериментальным путем обосновать применение механизма разрушения информации на основе неразрушающего устройство хранения метода (электрического изменения состояния электронной памяти) для разрушения информации с ограниченным периодом актуальности в мобильных устройствах хранения данных.

Литература

1. Бобрыкин С. Н., Рыжиков С. С. Термохимическое уничтожение носителей информации. http://www.bnti.ru/showart.asp?aid = 528 & lvl = 02.32.

2. Gutmann P. Secure Deletion of Data from Magnetic and Solid-State Memory // 6th USENIX Security Symposium Proceedings, San Jose, California, July 22–25, 1996. P. 77–89.