УДК 381.3

Анализ основных методов разрушения информации с целью определения оптимального механизма

Изложены результаты теоретических исследований применения механизмов разрушения для информации с ограниченным периодом актуальности в мобильных устройствах хранения.

**Ан. А. Ершов, В. Л. Ведерников,
Ал. А. Ершов, Д. Б. Николаев,
А. М. Шалыгин, А. И. Юрищев**

Введение

Целью данной работы является обоснование применения метода перезаписи для разрушения информации на мобильных устройствах хранения данных в ситуации, когда время, которым располагает нарушитель для восстановления информации, жестко ограничено. Достижение цели обеспечивается решением следующих задач:

– определение требуемой степени разрушения информации;
– разработка критериев применимости различных методов разрушения информации;
– анализ различных методов разрушения информации.

Поскольку разнообразие 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).

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

Многообразие возможных методов и путей разрушения информации ограничено только творческими способностями исследователей и современными техническими достижениями. Применимость различных методов ограничивается типом устройства хранения данных, его конструк-

тивными и эксплуатационными особенностями. Рассматриваемое 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.

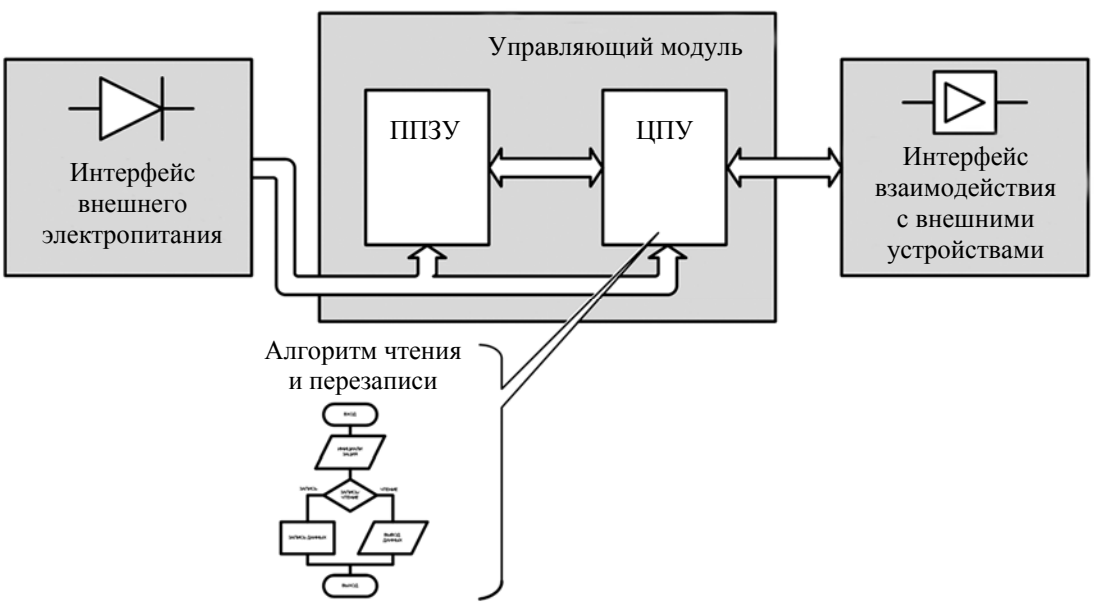

Рис. 1. Структура устройства хранения данных: ППЗУ – перепрограммируемое постоянное запоминающее устройство; ЦПУ – центральное процессорное устройство

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.

Разрушение информации в устройствах хранения данных может быть реализовано двумя принципиально различными путями:

– разрушение устройства хранения данных или его отдельных узлов;

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

Представленные варианты различаются 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.

Выбор пути разрушения информации может быть осуществлен на основании оценки времени, которым располагает нарушитель для восстановления информации, и технической оснащенности нарушителя средствами восстановления. Бесспорно утверждение о том, что гарантированное разрушение информации возможно только при разрушении непосредственного носителя информации, т. е. максимально возможная степень разрушения информации достигается разрушающими устройство хранения данных методами. Однако в случае ограниченности нарушителя жесткими временными рамками (имеющей место для информации с ограниченным период актуальности) предлагается ориентироваться при выборе метода разрушения информации на совокупность факторов, связанных с качественными эксплуатационными и технико-экономическими характеристиками мобильного устройства хранения данных, реализующего разрушение информации.

На основании вышесказанного требования к методу разрушения были сформулированы 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 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 должен обеспечивать степень разрушения, для которой время восстановления информации максимально эффективным методом на порядок больше времени, которым располагает нарушитель.

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 разделить их на 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 (далее – неразрушающим методам), основанным на перезаписи электронной памяти.

В основе методов механического разрушения лежит механический характер разрушающего воздействия на узлы устройства хранения данных, при этом источниками 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.

Рис. 2. Условное представление направлений исследований

В основе термохимического разрушения лежит явление самораспространяющегося высокотемпературного синтеза (СВС). Составы СВС способны обеспечить локальный разогрев устройства хранения данных до 3000 К 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 массива ячеек памяти при сохранении их работоспособного состояния.

Применение неразрушающих методов в ситуациях, когда нарушитель в своих действиях ограничен временными рамками, рассматривается как значительно более перспективное по сравнению с разрушающими методами.

2.2. Время разрушения информации

Механизм разрушения активируется владельцем, 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. Разрушающие методы имеют приблизительно равное относительно небольшое время разрушения информации (менее 1 с). Для специализированного 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 метода перезаписи информации. Аналогичная ситуация (наибольшего времени требует неразрушающий 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 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 возможность сконцентрировать разрушение на отдельных элементах [2] является общей для всех методов, разрушающих устройство, 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 включать осмотр всех элементов устройства на предмет разрушения, замену поврежденных элементов и полную проверку работоспособности отремонтированного устройства. В конечном счете для оценки объема ремонтных мероприятий для каждого метода необходима экспериментальная отработка устройств хранения данных, реализующих разрушение информации.

Преимуществом неразрушающих методов является отсутствие необходимости проведения 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

Сомнения в эксплуатационной безопасности могут вызывать термохимические и механические методы разрушения устройств хранения данных, т. е. методы, в которых источниками воздействия являются составы СВС и пиропатроны.

Здесь важно отметить факторы, которые обеспечивают высокий уровень эксплуатационной безопасности 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 том числе и электронных, устройствах продемонстрировала их эксплуатационную безопасность.

2.5. Массогабаритные характеристики

Наименьшими массогабаритными характеристиками обладает механизм неразрушающего метода разрушения информации, поскольку для реализации этого метода требуется незначительная схемотехническая доработка устройства хранения и его программного обеспечения.

Основным фактором, влияющим на увеличение массогабаритных характеристик устройства хранения данных при установке в него механизма разрушения информации на основе перезаписи, является внутренний источник электропитания относительно небольшой емкости (например, ионистор К58-6а-5,5В-0,68Ф диаметром 21 мм, высотой 9 мм и массой 11,6 г).

Немного большими массогабаритными характеристиками обладает механизм термохимического метода разрушения информации, что объясняется наличием брикета из состава СВС массой несколько грамм и размерами микросхемы памяти, а также наличием внутреннего источника электропитания (например, ионистора К58-4-2,5В-4,7Ф 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 крупных 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 (элемент, разрушающий корпус и кристалл микросхемы) 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. 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 техни-

ческого обслуживания этих устройств 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. Данный вывод сделан на основе следующих факторов:

– 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 [2];

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

3. Механизм разрушения информации на основе перезаписи

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;

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

Таким образом, применение метода перезаписи массива памяти для разрушения информации в условиях ограничения нарушителя жесткими временными рамками является более перспективным с точки зрения эксплуатационных и технико-экономических показателей.

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

Устройство хранения и разрушения информации путем перезаписи массива памяти (рис. 3) может быть построено на основе описанной выше конструкции устройства хранения данных путем некоторой доработки:

– 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.

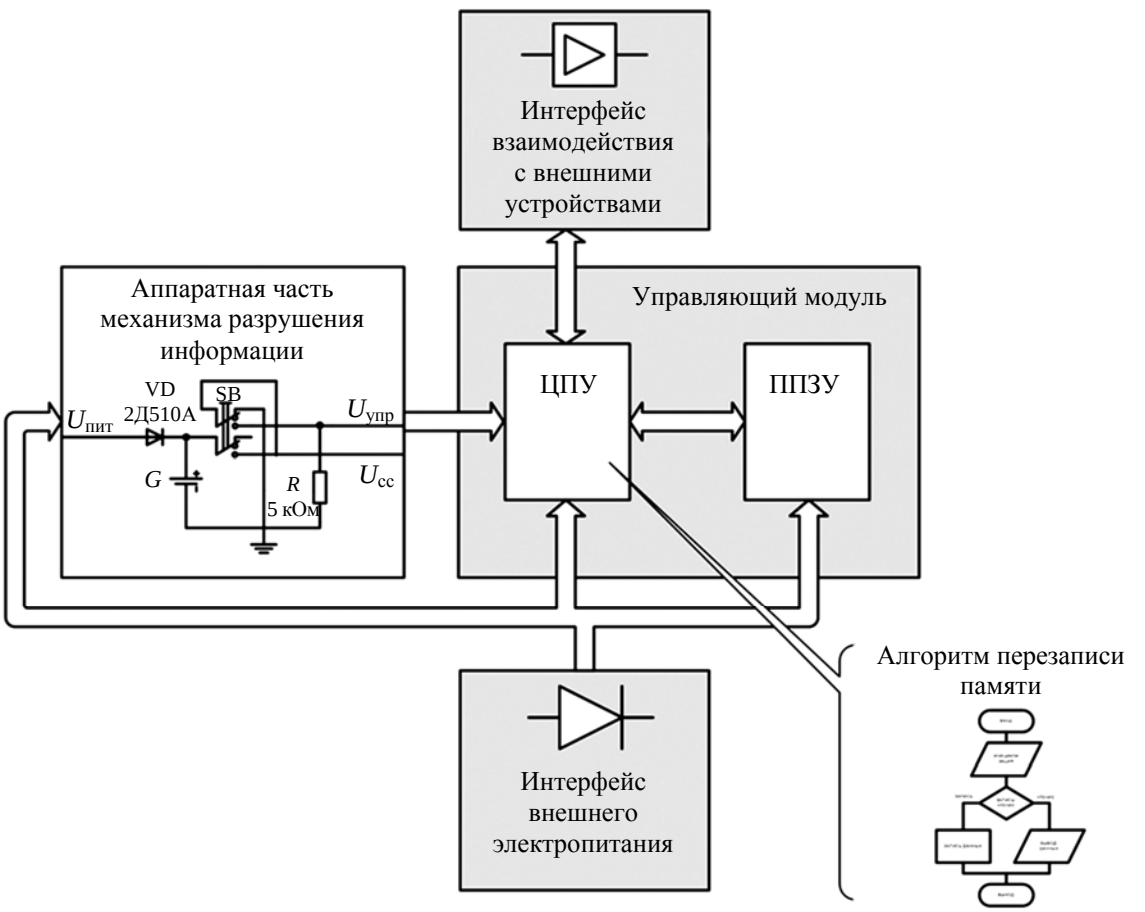

Рис. 3. Структура устройства хранения и разрушения информации

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 следующие 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, обеспечивающими:

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

– подключение электропитания от внутреннего источника $\left(U_{\text{сс}}\right)$ 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). Очевидно, что необходимая электрическая емкость источника энергии на несколько порядков меньше, чем номиналы емкостей источников тока, выпускаемых промышленностью, и, следовательно, несоизмерима с саморазрядом. Таким образом, емкость источника тока необходимо выбирать из условия недопущения саморазряда за время между циклами зарядки или периодом замены незаряжаемого источника электропитания.

Заключение

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

– концепция построения механизма разрушения информации в условиях ограниченного времени на восстановление разрушенной информации, ориентированная не на максимальную степень разрушения информации, а на достижение наилучших эксплуатационных и технико-экономических характеристик мобильного устройства;

– критерии анализа механизмов разрушения информации, разработанные на основе различных методов разрушения информации.

Разработка и анализ различных механизмов разрушения информации позволили расчетно-экспериментальным путем обосновать применение механизма разрушения информации на основе неразрушающего метода (перезаписи массива памяти) для разрушения информации с ограниченным периодом актуальности в мобильных устройствах хранения данных.

Список литературы

1. Ершов А. А., Николаев Д. Б., Шалыгин А. М. и др. Определение способа разрушения конфиденциальной информации с ограниченным периодом актуальности на мобильных устройствах хранения данных // Сб. тез. докл. X науч.-техн. конф. – Саров: РФЯЦ-ВНИИЭФ, 2011.

2. Бобрыкин С.Н., Рыжиков С.С. Термохимическое уничтожение носителей информации [Электронный ресурс]. – http://www.bnti.ru/showart.asp?aid=528&lvl=02.32.

3. Gutmann P. Data remanence in semiconductor devices // 10th USENIX Security Symposium [Electronical resource]. – http://www.usenix.org/events/sec01/full_papers/gutmann/gutmann.pdf.

4. Skorobogatov S. Data remanence in flash memory devices // Cryptographic Hardware and Embedded Systems Workshop (CHES-2005). LNCS 3659. P. 339–353.

5. Skorobogatov S., Anderson R. Optical fault induction attacks // Cryptographic Hardware and Embedded Systems Workshop (CHES-2002). LNCS 2523. P. 2–12

The Analysis of the Basic Destruction Methods of Information with the Purpose of Definition of the Optimum Mechanism

An. A. Ershov, V. L. Vedernikov, Al. A. Ershov, D. B.Nikolaev,
A. M. Shalygin, A. I. Urischev

Theoretical researches results of application of destruction mechanisms for the information with the limited period of a urgency in mobile devices of storage are stated.