**Задание пересылать мне на электронную почту:** [**param\_e@mail.ru**](mailto:param_e@mail.ru) **или через сайт техникума**

**Конспект лекции до 26.01.2022 (конспект в тетради; высылаете фотографии конспекта со своей подписью на каждом листе). Без подписи не принимаю конспект.**

**Ответы на вопросы в конце лекции, если они есть. (ответы в тетради после конспекта)**

**Сегодня две пары: 3 и 4.**

**3 пара - Подготовка конфиденциальных документов для архивного хранения и уничтожения**

**4 пара - Методы гарантированного уничтожения данных на жестких магнитных дисках**

**Лекции продублированы н аgoogle-диске по ссылке**

https://drive.google.com/drive/folders/1n\_kCtzoYTJCT8cLJ5ExZTnjEJvpDl3sW

**Подготовка конфиденциальных документов для архивного хранения и уничтожения (1 пара)**

Экспертиза ценность КД

Согласно Федеральному закону от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации» Архивный фонд Российской Федерации разделен на две составные части: государственную и негосударственную.

К *государственной* части Архивного фонда отнесены документы государственных и муниципальных органов власти и подведомственных им предприятий, а также документы предприятий смешанных форм собственности, в уставном капитале которых имеется преобладающая доля государственной собственности.

**Негосударственную** часть Архивного фонда составляют документы, находящиеся в собственности общественных и религиозных объединений и организаций или в частной собственности негосударственных объединений, организаций и физических лиц и представляющие собой историческую, научную, социальную, экономическую, политическую или культурную ценность.

Государственные и муниципальные органы власти и подведомственные им предприятия обязаны в установленном государственными нормативными актами порядке и в установленные сроки передавать документы постоянного хранения в государственные архивы. Негосударственные предприятия обладают правом собственности на созданные в процессе их деятельности документы, отнесенные к негосударственной части Архивного фонда, и могут передавать документы постоянного хранения в государственные архивы на основе соглашения (договора), оговаривая при необходимости особые условия хранения передаваемых документов и пользования ими.

Состав государственных и муниципальных органов власти и подведомственных им предприятий, передающих документы постоянного хранения в государственные архивы, а также категории передаваемых ими документов (все документы постоянного хранения или часть из них), определяются Федеральным архивным агентством (Росархивом) и органами управления архивным делом субъектов Российской Федерации. В отношении негосударственных предприятий такое определение производится органами и учреждениями Росархива совместно с собственниками документов и оформляется договором.

Таким образом, применительно к конфиденциальным документам источниками комплектования Архивного фонда РФ могут быть государственные и муниципальные органы власти и их предприятия, а также негосударственные предприятия, в деятельности которых образуются документы, составляющие служебную или коммерческую тайну.

Документы, составляющие коммерческую тайну государственных и негосударственных предприятий-источников комплектования Архивного фонда, могут передаваться в государственные архивы с согласия их собственников, но на практике такая передача осуществляется в исключительных случаях, обычно при ликвидации предприятий с отсутствием правопреемника. Если таких ситуаций не возникает, то документы передаются в государственные архивы, как правило, только после снятия с них грифа конфиденциальности, т.е. после того, как они перестают быть носителями коммерческой тайны.

При хранении КД должны быть обеспечены условия для физической сохранности и предотвращения утечки содержащейся в них информации. С целью уточнения или определения сроков хранения документов и отбора их на основе этих сроков для архивного хранения и уничтожения проводится экспертиза ценности документов.

Экспертиза ценности конфиденциальных документов проводится ежегодно или при небольшом объеме документов один раз в несколько лет, однако подвергать экспертизе целесообразно документы, изданные 35 лет назад, когда одновременно с подготовкой документов для архивного хранения возможны отбор их для уничтожения, так как значительное количество документов имеет срок хранения 35 лет.

Экспертизой ценности должны быть охвачены все конфиденциальные дела и документы выделенного хранения за соответствующий период времени, поскольку документы выделенного хранения являются составной частью документального фонда предприятия. К проведению экспертизы ценности конкретного дела (документа выделенного хранения) привлекаются члены ПДЭК, имеющие доступ к этому делу (документу).

Экспертиза ценности документов дела проводится путем изучения содержания каждого подшитого в дело документа и установления его соответствия сроку хранения и номерам статей перечня, указанным на обложке дела. Одновременно проверяется правильность формирования дела: соответствие видов и содержания документов заголовку дела, отсутствие в делах постоянного срока хранения документов временного срока хранения.

Экспертиза ценности документа выделенного хранения проводится путем изучения его содержания и определения срока хранения. Одновременно устанавливается возможность снятия грифа конфиденциальности с документов выделенного хранения, отдельных документов дела или с дела в целом. При определении или уточнении сроков хранения документов необходимо руководствоваться **Перечнем** типовых управленческих архивных документов, **Перечнем** научно-технической документации, образующихся в процессе деятельности организаций. Если на предприятии имеются документы, не предусмотренные названными перечнями и методическими рекомендациями, то срок их хранения следует определять на основе критериев оценки документов, к важнейшим из которых относятся:

- происхождение документа (место и время издания);

- содержание документа (значимость отображенного события, полнота его освещения, новизна, уникальность информации или ее повторяемость, целевое назначение документа);

- внешние особенности документа (подлинник или копия, характер резолюций, наличие помет, физическое состояние).

*Срок хранения дела в целом устанавливается по наивысшему сроку хранения документов, находящихся в деле*.

Результаты экспертизы ценности документов целесообразно фиксировать в рабочей карточке (тетради) эксперта с отражением в ней номера дела (документа выделенного хранения), его заголовка, операций (с обоснованиями), которые необходимо произвести: какие документы и в какое дело перешить, какие подлежат уничтожению, с каких можно снять гриф конфиденциальности, какими должны быть уточненный заголовок, срок хранения и номера статей по перечню.

По завершении экспертизы всех дел и документов выделенного хранения результаты работы всех экспертов рассматриваются на заседании ПДЭК и фиксируются в протоколе с отражением:

- какие дела и документы выделенного хранения (с уточненными заголовками, грифами конфиденциальности, сроками хранения и номерами статей по перечню) подлежат передаче на архивное хранение;

- какие документы из каких дел и в какие дела необходимо перешить;

- какие дела, документы из дел и документы выделенного хранения подлежат уничтожению;

- с каких дел, документов выделенного хранения или отдельных документов, подшитых в дела, должен быть снят гриф конфиденциальности с указанием в последнем случае, подлежит ли документ, с которого снимается гриф конфиденциальности, изъятию из дела или должен оставаться в нем.

Протокол заседания подписывается председателем и всеми членами ПДЭК и утверждается руководителем предприятия.

Подготовка КД и документов для архивного хранения

В соответствии с протоколом заседания ПДЭК сотрудниками подразделения конфиденциального делопроизводства производится частичное переформирование и дооформление соответствующих дел и документов выделенного хранения, в том числе:

- изъятие из дел документов, подлежащих перешивке в другие дела, и подшивка их в эти дела с проставлением в описях документов дел, из которых изъяты документы, их нового местонахождения и помещением в дела справок-заместителей, а также с перенумерацией листов перешитых документов в делах, в которые они помещены, внесением их в описи документов дел и исправлением количества листов в заверительной надписи дел, на обложках дел и в номенклатуре;

- изъятие из дел документов, подлежащих уничтожению;

- зачеркивание грифа конфиденциальности с проставлением даты и номера протокола заседания ПДЭК и своей подписи на документах, подшитых в дела, обложках дел и документов выделенного хранения, подлежащих рассекречиванию (в описях документов дела, номенклатуре и журнале учета документов выделенного хранения гриф конфиденциальности зачеркивается без ссылки на протокол заседания ПДЭК);

- изъятие из дел (по решению ПДЭК) документов, с которых снят гриф конфиденциальности, и передача их по акту в службу открытого делопроизводства с отметкой в описях документов дел и помещением в дела справок-заместителей;

- передача полностью рассекреченных дел и документов выделенного хранения по акту в службу открытого делопроизводства;

- корректировка заголовков, сроков хранения и номеров статей по перечню на обложках дел и в номенклатуре (на обложках дел дополнительно - крайних дат документов);

- проставление сроков хранения и номеров статей перечня на обложках документов выделенного хранения.

Если срок хранения дел и документов выделенного хранения установлен не **Перечнем**, а ПДЭК, то вместо статей перечня проставляется отметка ПДЭК.

*После изъятия из дел документов листы дела не перенумеровываются*.

На обложках дел и в номенклатуре рядом с количеством проставленных листов в скобках указывается количество листов, оставшихся в деле. В заверительной надписи дела под прежней надписью пишется: (прописью) листов изъято согласно записям в описи дела» с проставлением подписи, инициалов, фамилии лица, произведшего запись, и даты.

На дела и документы выделенного хранения, отобранные на архивное хранение, составляются раздельные по видам тайны описи. Описи дел и документов постоянного срока хранения имеют следующую форму.

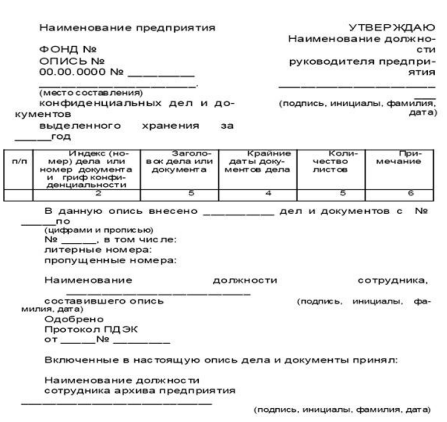


Рис. 1. Описи дел и документов постоянного срока хранения

На дела и документы временного хранения (свыше 10 лет) составляются аналогичные описи с добавлением перед «Примечанием» графы «Срок хранения и номера статей по перечню».

На научно-техническую, проектную, конструкторскую и иную специальную документацию составляются отдельные описи документов.

Грифы конфиденциальности описей дел должны соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках, дел и документов выделенного хранения. Если эти сведения не являются конфиденциальными, то грифы конфиденциальности описям не присваиваются. При наличии грифов описи регистрируются в журнале учета изданных документов.

Эта опись дополнительно утверждается протоколом экспертно-проверочной комиссии госархива. На дела и документы, не подлежащие передаче в госархив, опись составляется в двух экземплярах, если дела и документы передаются в архив предприятия, или в одном экземпляре, если не передаются. При передаче дел и документов в госархив или архив предприятия в подразделении конфиденциального делопроизводства остается один экземпляр описи с подписью сотрудника архива за получение включенных в опись дел и документов, остальные экземпляры передаются в архив.

Подготовка КД и документов для уничтожения

После утверждения описи дел и документов постоянного срока хранения составляется акт о выделении дел и документов за соответствующий период к **уничтожению**. В акт включаются отобранные ПДЭК для уничтожения дела, отдельные документы из дел и документы выделенного хранения. Гриф конфиденциальности акта должен соответствовать совокупной степени конфиденциальности сведений, содержащихся в заголовках, дел и документов. Если эти сведения не являются конфиденциальными, то гриф акту не присваивается. При наличии грифа акт регистрируется в журнале учета изданных документов.

Акт может иметь форму, указанную на рис 2. Отметки об уничтожении дел и документов в номенклатуре дел, журнале учета документов выделенного хранения и в описях документов дел произведены. Часть документов выделенного хранения (лишние экземпляры, справочно-информационные, присланные для сведения, отмененные), журналы (картотеки) учета конфиденциальных носителей, изданных документов, поступивших пакетов и документов могут включаться в данный акт или уничтожаться без рассмотрения ПДЭК по мере истечения сроков хранения по акту аналогичной формы (с исключением данных, относящихся к делам) без ссылки на протокол ПДЭК и без подписи ее председателя.

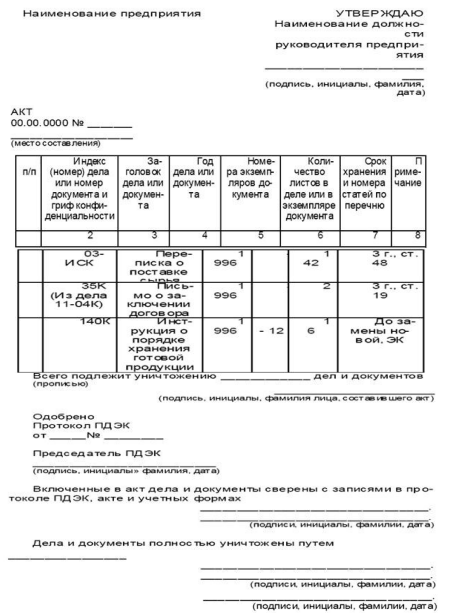


Рис. 2. Акт на уничтожение документов

Каждое дело, каждый документ и учетный журнал (картотека) вносятся в акт отдельной позицией и должны соответствовать данным о них, зафиксированным в протоколе ПДЭК и учетных формах. Если дело состоит из нескольких томов, то каждый из них включается в акт отдельной позицией.

При внесении в акт дел, из которых перед уничтожением были изъяты отдельные документы, указывается оставшееся в деле количество листов. Перед уничтожением включенных в акт дел, документов и учетных журналов (картотек) проверяется соответствие данных акта записям в протоколе ПДЭК, номенклатуре дел, журнале учета документов выделенного хранения, на обложках и в заверительных листах дел и документов выделенного хранения, в описях документов дела (по документам, изъятым из дела). Листы и учетные карточки просчитываются, сложенные документы разворачиваются. Соответствие данных заверяется в акте подписями проверявших. Уничтожение дел, документов и учетных журналов (картотек) производиться путем сжигания или с помощью бумагорезательной машины.

При уничтожении документов вне территории предприятия доставка их к месту уничтожения производится на служебном транспорте и принимаются меры, исключающие доступ к документам посторонних лиц. Отметки об уничтожении отдельных документов из дел проставляются в описях документов дел. Вместо уничтоженных документов в дела помещаются справки-заместители. Составление акта о выделении к уничтожению дел и документов и проставление в учетных формах отметок об их уничтожении осуществляются сотрудником подразделения конфиденциального делопроизводства. В проверке правильности включения в акт дел и документов и в их физическом уничтожении, кроме этого сотрудника, должен участвовать второй сотрудник.

**Методы гарантированного уничтожения данных на жестких магнитных дисках (2 пара)**

За последние несколько десятилетий компьютерные информационные технологии прочно вошли в нашу жизнь и стали составной частью документооборота. Первоначально отработанные механизмы обеспечения информационной безопасности для новых компьютерных систем уже не подходят, и требуют существенной модернизации. В первую очередь это касается отношения к информации, хранящейся на НЖМД.

Ранее для снятия информации с НЖМД был необходим физический доступ к носителю. Появление же компьютерных сетей создало новые угрозы безопасности информации, так как позволяет дистанционно, а иногда и скрыто от пользователя, получить доступ к хранимой на компьютере информации.

В настоящее время на развитие индустрии защиты информации (ЗИ), тратятся миллионы долларов. А по сути дела, решается одна задача – сделать открытую информацию доступной всем пользователям, а конфиденциальную – доступной только тому, кому она предназначается. Как в сфере бизнеса, так и в сфере государственного управления, уже скопились значительные объемы конфиденциальной информации, хранящиеся в базах данных персональных компьютеров. Эта информация представляет собой реальную ценность, а утечка ее в ряде случаев способна влиять даже на государственную безопасность.

Данное обстоятельство дало мощный толчок к развитию всевозможных программных и аппаратных средств добывания информации из ПК и компьютерных сетей. Особенно уязвимыми оказались сети, имеющие прямой выход в интернет.

Пути или каналы утечки информации, позволяющие несанкционированно и безнаказанно снимать копии с информации, непосредственно связаны с технологиями обработки, передачи и утилизации информации, хранящейся на НЖМД.

Утечка информации при замене НЖМД

Быстрое устаревание компьютерных технологий - это уже установившееся явление. Каждые два года (по закону Мура) ПК удваивают свою мощность. После смены двух поколений ПК не представляет собой никакой ценности и его нецелесообразно поддерживать технически и программно. Замена этих компьютеров может осуществляться разными способами:

1. *Перенос ПК на другое место***.** Часто замена ПК принимает форму переноса компьютера с места, изначально предназначенного для решения определенных задач, на рабочее место, требующее меньшей вычислительной мощности. После переустановки системы старый ПК можно будет использовать на новом месте как автоматизированную систему начального уровня.
2. *Продажа ПК как «second hand».* Даже если система не находит применения в организации, она может быть продана полностью или по частям учреждениям, которые могут использовать ее целиком или отдельные комплектующие (сервисные центры, начинающие пользователи и т.д.).
3. *Дарение ПК*. Очень часто старые ПК безвозмездно передаются детским учреждениям или благотворительным организациям.

*Во всех этих случаях старые ПК вывозятся вместе со всеми данными, в том числе и с КИ, на защиту которых были потрачены деньги и время, и это происходит в крупных организациях почти каждый день.*

В то время, как существуют не только законы, но и аппаратные средства, запрещающие или препятствующие получению конфиденциальной информации, снятие данных со списанного НЖМД позволяет заинтересованному лицу не только обойти системы безопасности без проявления внешних признаков, но и сделать это практически законно.

Многие руководители организаций и пользователи ПК не знают, что простое удаление файлов или даже переформатирование жесткого диска фактически не удаляет данные. Стоит только однажды записать информацию на НЖМД и удалить ее из магнитной памяти диска будет очень сложно.

Кроме той конфиденциальной информации, о которой знают пользователи (бухгалтерской, финансовой, личной, перспективных разработках), на ПК может храниться множество других конфиденциальных данных, которые не всегда известны оператору. Приложения и операционные системы (ОС) хранят пароли, ключи шифрования и другие данные с ограниченным доступом в различных местах, включая файлы конфигурации и временные файлы. Операционные системы произвольным образом записывают содержимое памяти в файл подкачки на диске, что не дает возможности узнать, что из этих данных действительно сохранено на носителе.

В настоящее время проблемой является и установленное программное обеспечение персональных компьютеров. Практически все лицензионное ПО не может передаваться без лицензий со старым аппаратным обеспечением. Поэтому требование по удалению лицензионного ПО при продаже или передаче устаревшего ПК остается.

Утечка информации при замене неисправного НЖМД

Еще одним и очень важным каналом утечки информации являются неисправные винчестеры (78% случаев потери данных виноваты аппаратные сбои НЖМД).

Большинство дисков ломаются в гарантийный период и могут быть заменены по гарантии при условии сохранности пломб и отсутствии механических повреждений или следов вскрытия. При этом считать информацию с диска, переписать ее на другой носитель или стереть не предоставляется возможным по причине неисправности НЖМД. Жесткий диск с информацией обменивается фирмой-продавцом на новый накопитель, а неисправный накопитель отсылается производителю или переводится на длительное хранение. Огромное количество информации, в том числе и конфиденциальной, попадает в руки лиц, доступ которых нежелателен.

Основные положения защиты информации, хранимой на НЖМД

Обеспечение надежного уничтожения корпоративной информации в конце жизненного цикла НЖМД требует тщательной проработки вопросов безопасности информации.

Удаление данных с НЖМД само по себе не обеспечивает защиты информации. Процесс ЗИ должен основываться на ряде согласованных методик, обеспечивающих в конечном итоге высокую вероятность уничтожения информации.

Хотя ни одна из методик не может гарантировать 100% надежность уничтожения информации, существуют основные положения и условия защиты информации.

1. *Необходимость физической защиты НЖМД*. Кража ПК или отдельных накопителей приводит к утечке информации, поэтому необходимо обеспечить их физическую сохранность с момента окончания срока эксплуатации до получения документированного подтверждения об уничтожении данных.
2. *Систематический контроль и ведение отчетности.* Систематический контроль подразумевает отслеживание выбывающих из эксплуатации накопителей, контроль процесса уничтожения информации и составление отчета об отклонениях в этом процессе и допущенных ошибках. Необходимо фиксировать следующие сведения:
   * уникальный идентификационный код уничтожаемого накопителя;
   * дату и время уничтожения;
   * ФИО исполнителя;
   * использованную методику уничтожения.

Способы уничтожения информации, хранимой на НЖМД

В настоящее время существует несколько способов уничтожения информации, хранимой на НЖМД. Уничтожение подразумевает стирание или удаление информации с жесткого диска таким образом, что ее невозможно восстановить ни обработкой на компьютерах с помощью специального ПО, ни с помощью лабораторных средств (например, [изучение поверхностей магнитных пластин](http://www.epos.ua/view/pubs_1?subaction=showfull&id=1027890000&archive=&start_from=&ucat=1&) с помощью сканирующей микроскопии).

Способы уничтожения информации на НЖМД делятся на три большие группы.

1. **Программные**, в основу которых положено уничтожение информации, записанной на магнитном носителе, посредством штатных средств записи информации на магнитных носителях. В случае уничтожения информации на НЖМД программным методом, он может быть повторно использован в других ПК, после инсталляции новой ОС и приложений. Уничтожение производится наиболее простым и естественным способом – перезаписью информации. Перезапись – это процесс записи несекретных данных в область памяти, где ранее содержались секретные данные.

Следует отметить очень важную деталь – при перезаписи информации работоспособность НЖМД полностью сохраняется, если он был полностью исправным. На изношенном или неисправном НЖМД провести надежное уничтожение информации невозможно.

1. **Механические**, связанные с механическим повреждением основы, на которую нанесен магнитный слой – физический носитель информации.
2. **Физические**, связанные с физическими принципами цифровой записи на магнитный носитель, и основанные на перестройке структуры магнитного материала рабочих поверхностей носителя. По способу воздействия на накопитель:
3. без разрушения гермокамеры и рабочих поверхностей НЖМД;
4. с разрушением НЖМД.

Программные способы уничтожения информации на НЖМД

1. **Начальный уровень (уровень 0).** Наиболее простая и часто применяемая форма уничтожения информации на НЖМД. Вместо полного очистки жесткого диска в загрузочный сектор, основную и резервную таблицы разделов записывается последовательность нулей.  
   Однако в этом случае данные на диске не уничтожаются, к ним усложняется доступ. Полный доступ к информации на НЖМД легко восстанавливается с помощью специального ПО, производящего анализ секторов диска (Norton DiskEdit, WinHex).
2. **Уровень 1.** Производится запись последовательности нулей или единиц в сектора данных. При этом уничтожается не только загрузочная область, но и данные.  
   Обычным пользователям в этом случае практически невозможно восстановить уничтоженную информацию. Тем не менее, существует возможность восстановления информации при стирании перезаписью. В основе ее лежат:
   * ошибки оператора и неправильное использование ПО.
   * отказ ПО перезаписывать все адресуемое пространство диска.
   * остаточная информация в дефектных секторах.
   * анализ зон остаточной намагниченности и эффекте краев дорожек.

Восстановить информацию, удаленную этим методом, стандартными средствами невозможно. Для восстановления требуются *специальные знания и оборудование*.

1. **Уровень 1+.** Используются несколько циклов перезаписи информации. Чем больше циклов перезаписи информации, тем сложнее восстановить удаленные данные. Это связано с неточностью позиционирования головки. Чем больше раз головка перезапишет данные, тем выше вероятность, что она сотрет зоны остаточной намагниченности на краях дорожки.  
   Последовательности, прописываемые в сектора данных, стандартизированы. Перезапись затрудняет процесс восстановления информации, но такая возможность остается. Для восстановления информации требуется очень дорогое и сложное оборудование и ПО.

*Выводы по программным методам уничтожения информации на НЖМД:*

Недостатки.

1. Низкая надежность уничтожения информации. После применения программных методов стирания информации перезаписью имеется возможность восстановления информации квалифицированным экспертом с помощью или без специальных средств.
2. Длительное время перезаписи информации носителя (десятки минут, часы). При многопроходной перезаписи время уничтожения информации для одного носителя умножается на количество проходов.
3. Перезапись информации возможна только на исправном НЖМД.

Достоинства.

1. Имеется возможность повторного использования НЖМД;
2. Низкая цена и стоимость эксплуатации ПО или специальных средств.

Механические методы уничтожения информации на НЖМД

Часто, когда необходима повышенная надежность уничтожения информации, к НЖМД применяют механические методы уничтожения, при которых разрушается сам носитель информации.

Стоимость накопителей на жестких дисках значительно снизилась за последние годы. Поэтому, как и в случае гибких магнитных дисков, для многих компаний может быть экономически целесообразно уничтожать их, а не удалять секретную информацию. Но здесь мы сталкиваемся с проблемой высокой стоимости оборудования для механического уничтожения и процессом контроля уничтожения в случае наличия этого оборудования.

Механические методы уничтожения информации подразделяются.

* **Механическое воздействия**. Измельчение носителя путем пропускания через устройство измельчения (шредер). НЖМД разрушается механически так, чтобы исключить возможность прочтения информации каким-либо способом с его рабочих дисков. При этом методе существует опасность, что при измельчении могут оставаться фрагменты, достаточно крупные, чтобы восстановить информацию в лабораторных условиях. Часто используемые на практике методы сверления отверстий и удары молотком по приводу на самом деле вовсе не уничтожают или уничтожают только малую часть информации.
* **Термические**. Нагревание носителя до температуры плавления в специальных печах.  
  При этом способе гарантия уничтожения информации наступает при разогреве носителя до температуры 800-1000°С. В этом случае информация становится абсолютно невосстанавливаемой по целому комплексу причин. Такой способ уничтожения информации может быть рекомендован для носителей, содержащих государственную тайну.
* **Пиротехнические**. Разрушение носителя взрывом.
* **Металлотермические**. Уничтожение подложки диска, непосредственно на которую нанесено магнитное покрытые, высокой температурой самораспространяющегося высокотемпературного синтеза (СВС). При этом на подложку в процессе производства наносится специальный слой термитного покрытия.
* **Химические**. Разрушение рабочего слоя или основы носителя химически агрессивными средами.
* **Радиационные**. Разрушение носителя ионизирующими излучениями.

В таблице представлены основные показатели механических методов уничтожения информации на НЖМД.

Таблица. Методы уничтожения информации на НЖМД

|  |  |  |
| --- | --- | --- |
| Механический | Измельчение носителя, его разрушение механическим воздействием. | Разрушающий метод. Возможно гарантированное уничтожение. |
| Термический | Нагревание носителя до температуры разрушения его основы (или до точки Кюри) | Разрушающий метод. Гарантированное уничтожение. |
| Пиротехнический | Разрушение носителя взрывом | Разрушающий метод. Возможно гарантированное уничтожение. Проблема обеспечения безопасности оператора. |
| Металлотермический | Уничтожение основы носителя высокой температурой самораспространяющегося высокотемпературного синтеза (СВС). | Разрушающий метод. Гарантированное уничтожение. |
| Химический | Разрушение рабочего слоя или основы носителя химически агрессивными средами. | Разрушающий метод. Гарантированное уничтожение. Проблема обеспечения безопасности оператора. |
| Радиационный | Разрушение носителя ионизирующими излучениями | Разрушающий метод. Опасность облучения. |

Одни из них экологически небезопасны, другие могут обеспечить высокую надежность уничтожения информации, но требуют настолько специфического и дорогостоящего оборудования, которое могут позволить себе лишь единичные корпоративные пользователи.

Во всех этих методах отсутствует возможность повторного использования НЖМД.

Физические методы уничтожения информации на НЖМД

В настоящее время оптимальным подходом для обеспечения надежности уничтожения информации без уничтожения носителя является использование физических средств, связанных с перестройкой структуры магнитного материала рабочих поверхностей носителя.

Для уничтожения информации на магнитных пластинах НЖМД необходимо устранить неоднородности вектора намагниченности участков рабочей поверхности, несущих информацию о предшествующих записях. Указанное изменение структуры поля вектора намагниченности магнитного слоя может быть выполнено несколькими принципиально различными способами.

*Размагничивание рабочих поверхностей носителя.* Размагнитить ферромагнетик можно и другим способом – поместить его в медленно убывающее переменное магнитное поле.

Более продуктивным является подход, связанный с намагничиванием рабочих поверхностей носителя до максимально возможных значений (насыщения) носителя.

*Намагничивание.* Способ основан на положении, что в случае НЖМД внешнее магнитное поле рассматривается как аналог поля, создаваемого магнитными головками при записи. Если характеристики внешнего поля будут превышать напряженность поля, создаваемого головками на такую величину, при которой произойдет магнитное насыщение материала поверхности диска, то все магнитные домены будут переориентированы по направлению этого внешнего поля и вся информация на НЖМД будет уничтожена.

**Выводы**

1. Размагничивание (намагничивание) – достаточно надежный метод уничтожения информации с поверхностей магнитных носителей при условиях:
   * правильного применения размагничивателей (намагничивателей) с полями достаточной напряженности;
   * обязательного применения средств визуализации магнитных полей носителя для контроля надежности уничтожения информации.