УНИЧТОЖЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Н.А. Храмцовская

ведущий эксперт по управлению документацией компании "Электронные Офисные Системы", член Гильдии Управляющих Документацией и ARMA International

См. статью Н.А.Храмцовской «Уничтожение и восстановление документов» на стр. 9 журнала № 12`2005. Автор анализирует на предмет эффективности и дороговизны четыре метода уничтожения бумажных документов, а потом рассказывает, какими способами их все-таки можно восстановить

В связи с развитием информационных технологий постоянно растут объемы информации и документации, хранящихся в организациях в цифровом виде. Постепенно совершенствуется законодательство и признается юридическая сила электронных документов. В итоге рано или поздно встает проблема, которую придется решать практически всем, – как правильно и надежно уничтожать электронные документы, когда нужда в них пропадает.

Необходимость своевременного уничтожения электронных документов вытекает из общих требований по защите информации и документации. Эти требования содержатся в законах и нормативных актах, которые:

- определяют порядок уничтожения деловых документов с истекшими сроками хранения (включая сообщения электронной почты);
- регулируют защиту "специфической" информации, к которой относятся: конфиденциальная и секретная информация, персональные данные;
- регламентируют вопросы обеспечения информационной безопасности организации, ее сотрудников и клиентов, в том числе уничтожение информации в отслуживших свое системах и носителях.

Проблемы уничтожения электронных документов

Основные сложности, возникающие при уничтожении электронных документов, связаны с особенностями цифровых носителей информации, а также с недостаточностью отечественной законодательно-нормативной базы. Среди многочисленных проблем можно выделить несколько наиболее острых.

Часто служба ДОУ не контролирует электронные документы, их хранение и уничтожение, – и результат не заставляет себя ждать. Правильно провести уничтожение можно лишь тогда, когда организация и сотрудники, отвечающие за эту работу, могут точно сказать, что, где и как хранится в электронных системах.

К сожалению, большинство организаций не в состоянии ответить на эти элементарные вопросы, поскольку в них за организацию работы с электронны-

ми документами отвечают либо все, либо никто. Чем больше накапливается электронной информации, тем больше хаос в хранении. Все делают вид, что проблемы не существует, но это помогает только до поры до времени.

Пример 1

В конце 90-х годов Управление операциями ЦРУ проводило миграцию сообщений электронной почты из устаревшей системы в Lotus Notes. Чтобы исключить потерю нужной информации, сотрудникам пришлось просмотреть более миллиона документов. Сохраняемые документы либо распечатывались, либо преобразовывались в формат, воспринимаемый новой системой. Проводя в 2000 году аудит делопроизводства и документооборота в ЦРУ, Национальные Архивы США выделили этот случай как яркий пример того, как отсутствие постоянного ежедневного управления документами приводит к огромным расходам.[1]

Розыск и уничтожение всех копий электронных документов – еще более "злобная" проблема.

Пример 2

По подсчетам службы ДОУ одного из крупных американских университетов, в случае "всеобщей" рассылки какого-либо документа персоналу и студентам в электронных системах будет сохранено не менее тысячи его копий (примерно 10% от общего объема рассылки).

Большинство электронных документов распространяется в виде неконтролируемых копий. Это означает, что никто в организации не знает, где и сколько экземпляров документа может храниться. Из-за этого обеспечить уничтожение всех копий (включая данные на резервных носителях) очень сложно. Для этого нужны хорошо продуманные организационные меры и исполнительская дисциплина. Такое положение вещей значительно повышает риски сохранения лишней и ненужной информации и приводит к перерасходу ресурсов информационных систем.

Современные электронные ***носители информации*** достаточно "хрупки", – но, как ни странно, очень часто они ***проявляют потрясающую живучесть***. Конечно, когда удается восстановить вроде бы безнадежно потерянную информацию с отказавшего носителя, это большая радость для его владельца. Но если задача состоит в том, чтобы окончательно и бесповоротно уничтожить данные, то это качество может создать проблему для служб ИТ и ДОУ.

Пример 3

В феврале 2003 года потерпел катастрофу шаттл "Колумбия". Среди обломков корабля, извлеченных спустя несколько дней из озера, были найдены "останки" двух ноутбуков. Американская фирма Kroll Ontrack (одна из двух ведущих компаний, специализирующихся на восстановлении данных) восстановила 99% содержимого их жестких дисков.[2]

[1] http://www.fas.org/sgp/othergov/naracia.html (ссылки проверены 20 февраля 2006 г.)
[2] http://directory.eoportal.org/pres_FREESTARonShuttleFlightSTS107.html

Пример 4

После урагана "Катрина", от которого в 2005 году серьезно пострадал город Нью-Орлеан в США, многие фирмы и частные лица извлекли жесткие диски из своих компьютеров, "проплававших" почти месяц в грязной морской воде, и послали их на восстановление. В общей сложности удалось восстановить информацию с 90% жестких дисков, доставленных с места катастрофы. Средняя стоимость восстановления данных с одного жесткого диска составила тысячу долларов США.

Постоянно растет число видов носителей, которые нужно контролировать. Это не только привычные дискеты, CD, DVD и жесткие диски, но и, например, флэш-память в многочисленных портативных устройствах, сим-карты телефонов, смарт-карты и т.п. В подавляющем большинстве отечественных организаций не существует даже примерного списка носителей, на которых может оказаться корпоративная электронная информация.

Сим-карта отслужившего свое телефона может содержать телефонные номера сотрудников, партнеров и клиентов компании, а также конфиденциальные SMS-сообщения. Современные цифровые фотоаппараты, MP3-плееры и другие устройства вполне могут использоваться не только по прямому назначению, но и для переноса информации.

Сложнее всего уничтожать информацию, которая находилась на компьютере, подключенном к глобальной или локальной сети. ***Легкость распространения электронной информации просто поражает воображение***. То, что хотя бы ненадолго было выложено организацией в ***Интернете*** в свободном доступе, может остаться там навсегда, даже если, спохватившись, собственник информации удалил ее со своего сайта.

Пример 5

Секретный документ о прослушивании и записи телефонных разговоров Министерства обороны Нидерландов оказался выложен в сеть сотрудником министерства, который по ошибке разместил его в папку общего доступа файлообменной сети.[3]

Пример 6

В декабре 2005 года коды доступа на территорию 16 японских аэропортов, включая столичные, а также американского аэропорта на острове Гуам, «утекли» с зараженного вирусом домашнего компьютера пилота компании Japan Airlines (JAL) и были опубликованы в Интернете. [4]

Пример 7

В начале февраля 2005 года несколько тысяч секретных документов, принадлежащих Департаменту внутренней безопасности США (Department of Homeland Security), оказались доступными для пользователей поисковой системы Google. "Прокололось" Министерство энергетики США, выложив секретную документацию в разделах своего сайта, которые индексировались поисковой системой. В результате документы стали доступны всем желающим. Даже после того, как это было обнаружено и документы с сайта были удалены, уничтожить их полностью стало невозможно, т.к. они сначала были

сохранены как образы страниц на серверах Google, а потом начали размножаться и размещаться в сотнях экземплярах по всему миру. [5]

Развитые методы электронной судебно-криминалистической экспертизы, наличие специального оборудования и программного обеспечения ***увеличивают риски восстановления уничтоженных материалов***. Во многих странах мира уже сейчас успешно действуют специализированные компании по восстановлению данных и проведению компьютерной судебной экспертизы, когда информация восстанавливается таким образом, чтобы ее можно было использовать в качестве доказательства в судебных разбирательствах.

Пример 8

Исследования, проведенные Агентством Национальной Безопасности США (самой "закрытой" и наиболее финансируемой американской спецслужбой, специализирующейся на "электронной разведке"), показали, что осмысленную информацию удается восстановить даже с фрагментов измельченного жесткого диска размером 1 х 1 мм.[6]

Принципы и методы уничтожения электронных документов

Гарантированное уничтожение информации возможно только вместе с носителями. Об этом говорит многовековой опыт, это же сейчас подтверждают и специалисты по информационной безопасности, которые в один голос говорят, что любые попытки повторного использования носителя значительно повышают риски утечки информации. Кроме того, многие пользователи не знают или не принимают во внимание, что *простое удаление файлов или даже переформатирование носителя (жесткий диск, флоппи-диск и т.д.) не гарантируют того, что данные не будут восстановлены.*

Пример 9

Эксперимент по изучению того, какая информация остается на списанных жестких дисках, был проведен студентами Гарфинкелем и Шелатом. Студенты закупили 158 б/у жестких дисков и проверили их на читаемость. Они также проанализировали содержание 129 читаемых дисков и получили следующий результат: полностью были "очищены" только 9%, в 64% не была уничтожена файловая система. На трети дисков были обнаружены номера кредитных карт, а два из них содержали тысячи номеров кредитных карт. Попался и диск из банкомата – со всем его математическим обеспечением и контрольной информацией.[7]

---

[3] http://www.svoboda.org/ll/sci/0205/ll.021605-2.asp
[4] http://www.securitylab.ru/news/242842.php
[5] http://www.infowatch.ru/threats?chapter=147151398&id=177986123
[6] http://www.snia.org/education/tutorials/fall2005/security/Data_Disposal_Gone_for_Good_Rev3.pdf
[7] Simson Garfinkel, Abhi Shelat "Remembrance of Data Passed: A Study of Disk Sanitization Practices", IEEE Security & Privacy, vol.1, no.1, 2003, http://www.cs.unibo.it/~montreso/doc/papers/AStudyOfDiskSanitizationPractices.pdf

Регулярно “всплывают” яркие примеры последствий подобного отношения к электронной информации, но число “умников” от этого не уменьшается.

Пример 10

В Польше в апреле 2004 года журнал «Не» анонсировал ряд материалов о внутренней жизни польского Министерства иностранных дел – «когда, кто, с кем и за сколько». При этом журнал опирался на информацию, полученную с жестких дисков компьютеров МИД, попавших в редакцию.

Расследование, проведенное Агентством внутренней безопасности Польши (АВБ), показало, что технический сотрудник МИД Польши вынес из министерства 12 жестких дисков и продал их по 10 злотых за штуку (около $3) фирме, занимающейся утилизацией старого компьютерного оборудования. Фирма не поленилась проверить содержание дисков и затем предложила «сенсационный материал» всей польской прессе.

Документы содержали информацию (в том числе и секретную, и отнесенную к государственной тайне) о деятельности польского МИД в 1992 – 2003 годах. «На множестве документов стоит дата, многие из них с грифом «секретно», – подчеркивалось в публикации. В документах содержалась и персональная информация о сотрудниках министерства, например, о номере паспорта министра иностранных дел, его группе крови, стоимости фрака министра, детальном поминутном графике встреч. Среди документов – отчеты с секретных заседаний министерства, касающиеся очередных тендеров на покупку военной техники, и многое другое.[8]

Стандарты об уничтожении информации с электронных носителей

Любое уничтожение документов, независимо от вида носителя информации, должно быть проведено, основываясь на определенных принципах, которые зафиксированы в ***международном стандарте по управлению документацией ISO 15489***. *Принципы физического уничтожения документов* (стандарт ISO 15489-1:2001):

- уничтожение всегда должно быть санкционированным,
- запрещается уничтожать документы, имеющие отношение к идущему или предвидимому разбирательству по судебным искам или расследованию,
- уничтожение документов должно проводиться с сохранением конфиденциальности содержащейся в них информации,
- должны быть уничтожены все копии документов, отобранных на уничтожение, включая страховые копии, резервные копии и копии для длительного хранения.

В мире существует ряд хороших стандартов и методик, описывающих правила и процедуры надежного уничтожения документов и информации на различных видах электронных носителей.

Методика уничтожения информации на оптических носителях описана в ***техническом отчете ISO/TR 12037:1998***, “Electronic imaging — Recommendations for the expungement of information recorded on write-once optical media” (“Сканирование и электронная обработка документов – Рекомендации по уничтожению информации, записанной на оптических носителях однократ-

ной записи"). Этот стандарт довольно "старый", принят еще в прошлом веке, в 1998 году. Он рассматривает достаточно узкую проблему частичного уничтожения информации на носителе однократной записи.

В США широко используется ***руководство по обеспечению безопасности в промышленности DoD 5220.22-M (NISPOM)***, разработанное совместно Министерствами обороны, энергетики, Комиссией по атомной энергии и ЦРУ[9]. Одна из глав этого руководства содержит сводную таблицу (Clearing and Sanitization Matrix) по "очистке" носителей информации, в которой перечислены методы уничтожения для разных видов носителей. Руководство NISPOM предлагает два основных метода уничтожения для электронных документов:

- *размагничивание* (для лент и магнитных дисков), или
- *уничтожение путем дезинтеграции, сжигания, пульверизации, шредирования или расплавления* (для всех видов носителей информации).

В феврале 2006 года Национальный институт стандартов и технологии США опубликовал ***проект руководства по очистке носителей информации NIST SP 800-88***[10]. Данное руководство описывает общие принципы организации уничтожения информации, обязанности и ответственность должностных лиц. Даются рекомендации по методам уничтожения информации на разнообразных современных видах носителей. Процессы "очистки" носителей информации разделены в руководстве на четыре группы:

- *выбрасывание* (disposal) – носители выбрасываются или идут на переработку без какой-либо специальной обработки (пример – сдача на переработку бумажных документов, не содержащих конфиденциальной информации);
- *стирание информации* (clearing) – уровень очистки носителей, защищающий конфиденциальную информацию от попыток ее восстановления при помощи обычных программно-аппаратных средств (keyboard attack). Перезапись информации является приемлемым методом;
- *вычищение информации* (purging) – уровень очистки носителей, защищающий конфиденциальную информацию от попыток ее восстановления при помощи специального оборудования и программных средств (laboratory attack) и специально обученного персонала. В частности, приемлемыми методами являются размагничивание (degaussing) и использование (для жестких дисков ATA) поставляемых производителем оборудования программ безопасного стирания информации на жестких дисках;
- *физическое уничтожение*. Методы: дезинтеграция, сжигание, пульверизация, расплавление, шредирование, удаление слоя-носителя информации при помощи абразивных материалов.

---

[8] http://www.ckandal.info/main.html?news=1159 , http://oldnews.mail.ru/news.html?456137

[9] DoD 5220.22-M «National Industrial Security Program Operating Manual (NISPOM)» (Includes Change 1, July 31, 1997),Department of Defense - Department of Energy - Nuclear Regulatory Commission - Central Intelligence Agency, January 1995, http://www.usaid.gov/policy/ads/500/d522022m.pdf (см. 8-306 Maintenance)

[10] Matthew Scholl, Richard Kissel, Steven Skolochenko, Xing Li «Coputer Security - Guidelines for Media Sanitization (Public Draft)» ("Компьютерная безопасность – Руководство по очистке носителей информации (проект для публичного обсуждения)"), NIST Special Publication 800-88, National Institute of Standards and Technology, February, 2006, http://csrc.nist.gov/publications/drafts/DRAFT-sp800-88-Feb3_2006.pdf

Технические средства и приемы для уничтожения электронных документов

Сейчас даже не очень опытные пользователи обычно знают, что нажатие кнопки “Delete” вовсе не означает, что информация “испарилась” с носителя, хотя компьютер и извещает об успешном удалении файла. Это только кажущееся уничтожение информации, т.к. уничтожаются не сами документы, а ссылки на них. Если стираемая информация не имеет особой ценности, то риск, связанный с возможностью ее восстановления, невелик. Если же речь идет о конфиденциальной информации, то в этом случае хотелось бы быть уверенным в надежности ее уничтожения.

Выбирая тот или другой способ уничтожения, необходимо провести оценку рисков и дать ответы на следующие вопросы:

- Какова вероятность утечки информации при выбранном методе уничтожения?
- Во сколько обойдется организации тот или иной метод уничтожения?
- Какие затраты нужны для восстановления уничтоженной информации?
- Каковы могут быть для организации последствия в случае восстановления документов?

В зависимости от полученных ответов организация может выбрать один из перечисленных ниже способов.

Способ 1: ***Уничтожение с использованием специального программного обеспечения***, которое уничтожает информацию методом перезаписи или стирания. Для более надежного уничтожения информации эта процедура проводится многократно.

Недостатки:

- Надежность уничтожения информации не слишком высокая, поскольку остается возможность восстановления информации высококвалифицированными специалистами в лабораторных условиях, с использованием специального оборудования и программ. Современные методы позволяют восстанавливать информацию, уничтоженную в результате многократной перезаписи, в том числе и с отдельных фрагментов носителя.
- Специалисты по защите информации рекомендуют проводить перезапись не менее 7 раз, а некоторые уверяют, что надежное уничтожение обеспечивает 35-кратная перезапись. Процесс уничтожения требует значительного времени даже при использовании имеющихся специальных аппаратных средств. С учетом оплаты труда квалифицированных специалистов подобная “очистка” морально устаревшего носителя для повторного использования может оказаться для организации экономически невыгодной.
- Если носитель неисправен или содержит нечитаемые зоны, перезапись может не справиться со своей задачей.

Достоинства:

- Носитель сохраняется и может быть повторно использован. Это выгодно, когда его стоимость высока.
- Стоимость соответствующего программного обеспечения и специального оборудования достаточно низкая, что позволяет использовать этот метод и в небольших организациях.

Многие государственные и коммерческие структуры сталкиваются с проблемой утилизации устаревшего компьютерного оборудования. Попытки сэкономить (или же произвести благоприятное впечатление на общественность, передав устаревшее оборудование на благотворительные цели) порой могут привести к весьма печальным последствиям.

Пример 11

В конце 2000 г. в школы США было решено передать более 74 тыс. единиц списанной из организаций Министерства обороны компьютерной техники на сумму 60 млн. долларов. В январе 2001 г., после того, как на ряде прошедших очистку жестких дисков обнаружились восстановимые конфиденциальные материалы, последовал приказ о физическом уничтожении всех жестких дисков. Только через пять месяцев это весьма непопулярное решение было отменено. По словам представителей Пентагона, они нашли способ защитить информацию, хранящуюся на жестких дисках устаревших компьютеров, которые военное ведомство намерено передать в средние школы США. Было решено уничтожить жесткие диски только на тех компьютерах, на которых ранее обрабатывалась секретная информация, а остальные просто переформатировать. [11]

Фрагмент документа

В начале 2005 года Национальная ассоциация по уничтожению информации (NAID) объявила, что она не рекомендует пользоваться для удаления данных с жестких дисков одними только чистящими программами. Исполнительный директор NAID Боб Джонсон сказал, что его организация и рада бы порекомендовать инструменты для уничтожения данных, но испытания оставляют сомнения в надежности чистящих продуктов. “Наша окончательная позиция заключается в том, что мы даем гарантию только при физическом уничтожении жесткого диска, – сказал Джонсон. – А если не сделать это надлежащим образом, то и физическое уничтожение может не дать нужного результата”.[12]

Информация и документы на носителях однократной записи (носители типа WORM, магнитооптические диски, CD-ROM, CD-R, оптические ленты) могут быть уничтожены методом стирания. Трудности могут возникнуть при необходимости только частичного уничтожения содержащейся на них информации, т.к. может быть поставлена под сомнение аутентичность и целостность всех оставшихся на носителе документов в том случае, если процесс уничтожения не был выполнен и задокументирован в соответствии с установленными процедурами. В некоторых системах однократной записи выборочное уничтожение трудно или невозможно реализовать. Тогда одним из решений может быть копирование сохраняемых документов на новый носитель и физическое уничтожение старого носителя информации.

Способ 2: ***Воздействие на рабочую поверхность носителя магнитным полем (размагничивание)***. Этот метод довольно широко известен и применяется для очистки магнитных носителей информации. Принцип действия приборов, с помощью которых проводится уничтожение информации, основан на размагни-

[11] http://www.utro.ru/news/2001060810125118596.shtml
[12] http://www.dialog-21.ru/full_digest.asp?digest_id=42051

чивании носителей под действием кратковременного электромагнитного импульса большой мощности. Метод применим к следующим видам носителей:

- жесткие диски,
- аудио- и микрокассеты,
- видеокассеты форматов Video-8, Hi-8, S-VHS-C, VHS-C,
- дискеты 3,5`` и 5``,
- картриджи с магнитной лентой.

Достоинства:

- приборы выпускаются разной производительности, вплоть до карманных и переносных вариантов;
- использование размагничивающих устройств не требует специальных навыков, т.к. требуется только установить носитель в прибор;
- процесс уничтожения происходит очень быстро.

Недостатки:

- повторное использование размагниченных жестких дисков невозможно;
- требуется специальное оборудование;
- сложно проверить и подтвердить надежность уничтожения информации на жестких дисках. Дело в том, что при размагничивании обычно выходит из строя внутренняя "начинка" жесткого диска. В то же время, если мощность магнитного поля недостаточна или если диск был неправильно вставлен в размагничивающее устройство, – в лабораторных условиях информация может быть частично восстановлена. Каждое новое поколение жестких дисков становится все более устойчивым к воздействию магнитного поля, и оборудование, надежно очищавшее старые диски, может уже не столь хорошо обрабатывать более новые модели;
- кажущаяся безвредность данного метода обманчива. Не случайно в соответствующих руководствах рекомендуется держать подальше от размагничивающих устройств не только электронные приборы или механические часы, но и людей, у которых вживлен электрокардиостимулятор.

Говоря о методах "очистки" информации, хочется еще раз подчеркнуть, что к тому времени, когда у организации возникает необходимость провести обновление компьютера и заменить его жесткие диски – это, как правило, уже морально устаревшее оборудование с небольшой остаточной стоимостью, повторное использование которого окупается только в качестве запчастей для все еще сохраняемых "на ходу" устаревших систем. Именно поэтому все чаще и чаще организации прибегают к механическому уничтожению жестких дисков.

Способ 3: ***Механическое уничтожение носителя вместе с информацией*** проводится тогда, когда требуется повышенная надежность уничтожения документов. Существует несколько наиболее широко применяемых методов:

- *Шредирование или измельчение* – наиболее популярный метод, в результате которого носитель измельчается в специальных устройствах.
- *Механическое воздействие* с помощью молотка или любого другого прибора, позволяющего пробить в носители дыры и т.д. Это не самый надежный метод, и в лабораторных условиях большую часть информации обычно можно восстановить.
- *Расплавление носителя* – требует специального оборудования. Обычно применяется для уничтожения секретной информации.
- *Использование химикатов,* когда магнитная пластина заливается специ-

альным химическим составом, а после такого "купания" еще для верности промывается ацетоном.

У механических способов уничтожения также есть свои плюсы и минусы.

Достоинства:

- дешевизна;
- уничтожение проходит быстро и наглядно, его можно зафиксировать не только документально, но и другими методами (фотография, видеозапись);
- если технология процесса уничтожения выдерживается, то восстановить информацию практически невозможно.

Недостатки:

- как правило, требуется специальное оборудование, при работе с которым необходимо соблюдать меры безопасности;
- повторное использование носителя невозможно.

Способ 4: ***Технологии "управления авторскими правами"*** дают возможность сделать нечитаемыми даже документы, находящиеся вне сферы контроля организации. При пересылке информации конкретному адресату ее можно защитить от дальнейшего распространения, копирования или печати с помощью технологии управления авторскими правами на информацию (IRM). Получателю можно предоставить права просмотра, рецензирования или редактирования документа, даже установить срок действия сообщения, по истечении которого документ невозможно будет просмотреть или изменить.

С одной стороны, подобные способы защиты и уничтожения информации могут иметь катастрофические последствия для электронного делопроизводства, если, например, в результате будет уничтожен документ, необходимый организации для защиты ее интересов в суде или в ходе расследования. С другой стороны, использование подобных технологий может позволить решить проблему неконтролируемых копий.

Проблема IRM-технологий – это проблема сегодняшнего дня, поскольку соответствующие средства уже появились и в Adobe Acrobat, и в Офисе компании Микрософт.

Экзотические способы уничтожения. Каждый раз, когда перед человечеством встает какая-либо серьезная проблема, сметливость и сообразительность отдельных индивидуумов просто поражает. Необходимость найти способы уничтожения информации подвигло многие умы на разработку экзотических методов с применением подручных средств. Часто практикуется использование носителей в качестве "тарелочек" для стрельбы, измельчение отдельных деталей в миксерах и кухонных комбайнах, запекание в индукционных печах (достаточно популярный, но небезопасный метод уничтожения CD и DVD-дисков). И это только маленькая толика вариантов, позволяющих избавляться от информации и ее носителей в домашних условиях!

Документирование уничтожения электронных документов

Любое уничтожение документов, независимо от вида носителя, должно тщательно документироваться – так же, как документируется уничтожение бумажных документов.

Начать стоит с разработки регламента по уничтожению электронных документов. Это позволит (или, наконец, заставит!) проанализировать состояние дел в организации со всеми ее электронными богатствами и продумать комплекс необходимых мер (организационных, технических и т.д.). В таком документе необходимо распределить ответственность за проведение работы, особенно если различные виды носителей обрабатываются и хранятся в различных подразделениях и отсутствует их централизованный учет.

Важно задокументировать весь ход уничтожения. Поскольку в нашей стране отсутствует не только соответствующая законодательно-нормативная база, но и методические рекомендации, то рекомендуется зафиксировать, кто, когда, каким способом провел уничтожение, кто выполнил проверку и т.д. В ответственных случаях помимо оформления актов можно сделать фотографии или видеозапись процесса уничтожения. Особое внимание стоит обратить на все случаи несоблюдения технологии уничтожения (включая документирование), а также на факты неполного уничтожения информации. Выявленные недостатки должны как можно скорее исправляться.

Восстановление электронных документов

Развитие информационных технологий вряд ли позволит "почивать на лаврах". Вечное соперничество брони и снаряда никогда не прекращается. Одни стремятся уничтожить информацию и документы, а другие – ищут способы восстановления. Об этом всегда нужно помнить при выборе методов уничтожения в каждой конкретной ситуации.

В настоящее время рынок услуг по восстановлению данных активно развивается. Такие фирмы есть и в нашей стране. Спрос на подобные услуги растет с каждым годом, делая этот вид деятельности весьма доходным. Объем мирового рынка услуг восстановления данных оценивается в 500 – 750 млн. долл. В год в фирмы, занимающиеся восстановлением данных, поступает примерно 300 тысяч носителей (1/1000 от ежегодного объема продаж жестких дисков).

* * *

Выбор метода уничтожения должен основываться на учете возможных рисков, связанных с восстановлением документов, и стоимости уничтожения. Необходимо постоянно совершенствовать используемые в организации технологии, поскольку появляется все больше и больше разнообразных носителей, которые имеет смысл "взять на карандаш".

Для специалистов в области управления документацией участие в уничтожении электронной информации – правильный, хотя и непростой шаг. Чем больше вопросов, связанных с электронными документами и информацией будут решаться с участием специалистов ДОУ, тем больше у них появится возможностей для карьерного и профессионального роста. На рынке труда уже сейчас ощущается дефицит специалистов, имеющих практический "делопроизводческий" опыт работы с электронными документами.