УДК 658.5

УНИЧТОЖЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Акулич Ю.И.

Учреждение образования «Белорусский государственный экономический университет», г. Минск, Республика Беларусь, e-mail a.yury@mail.ru

Необходимость своевременного уничтожения электронных документов вытекает из общих требований по защите информации и документации. Эти требования содержатся в нормативных правовых актах. В статье описаны методы уничтожения документов риски с этим связанные, а также необходимость постоянно совершенствовать используемые в организации технологии, поскольку появляется все больше и больше разнообразных носителей.

Необходимость своевременного уничтожения электронных документов вытекает из общих требований по защите информации и документации [1]. 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.

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. 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.

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

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.

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.

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.

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.

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

– 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*, «Сканирование и электронная обработка документов – Рекомендации по уничтожению информации, записанной на оптических носителях однократной 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. Одна из глав этого руководства содержит сводную таблицу 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). [2].

Национальный институт стандартов и технологии США разработал проект руководства по очистке носителей информации NIST SP 800-88. 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* – носители выбрасываются или идут на переработку без какой-либо специальной обработки (пример – сдача на переработку бумажных документов, не содержащих конфиденциальной информации);

– *стирание информации* – уровень очистки носителей, защищающий конфиденциальную информацию от попыток ее восстановления при помощи обычных программно-аппаратных средств.

– *вычищение информации* – уровень очистки носителей, защищающий конфиденциальную информацию от попыток ее восстановления при помощи специального оборудования и программных средств и специально обученного персонала. В частности, приемлемыми методами являются размагничивание и использование программ безопасного стирания информации на жестких дисках;

– *физическое уничтожение*. Методы: дезинтеграция, сжигание, пульверизация, расплавление, шредирование, удаление слоя-носителя информации при помощи абразивных

материалов.

Выбирая тот или иной способ уничтожения, необходимо провести оценку рисков и принять во внимание следующее:

– вероятность утечки информации при выбранном методе уничтожения

– затраты организации на применение того или иного метода уничтожения

– затраты на восстановление уничтоженной информации

– последствия для организации в случае восстановления документов

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

Начать стоит с разработки инструкции по уничтожению электронных документов, это позволит 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.

В настоящее время разработана технология, которую порой называют «*цифровым шредированием*» (digital shredding) [2]. Процесс цифрового шредирования прекрасно решает задачу удаления одних документов при одновременном сохранении других, делая «удаленные» документы нечитаемыми и невосстановимыми. Работает это следующим образом: документы шифруются во время их записи на WORM-носитель. При извлечении документов и получении к ним доступа они автоматически расшифровываются. Управление ключами шифрования увязано со сроком хранения документов: как только срок хранения истек, ключи уничтожаются. При использовании ключей достаточной длины восстановить ключ шифрования с использованием имеющихся в настоящий момент средств невозможно.

Результат аналогичен измельчению бумаги в конфетти или, скорее, ее пульверизации. Это даже почти аналогично размагничиванию лент перед повторным использованием. Если размагничивание провести как надо, то маловероятно, что средствами судебной экспертизы с лент удастся извлечь какую-то информацию. Основная разница между цифровым шредированием и размагничиванием заключается в том, что место на носителе повторно использовать не удастся, как в случае размагничивания ленты.

Еще раз следует отметить, что 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» [3].

Список литературы:

1. Храмцовская, Н. А. Уничтожние электронных документов / Н.А. Храмцовская //Делопроизводство и документооборот на предприятии. – 2006. – №3. – С.52-62

2.Технология и автоматизация делопроизводства: учеб. пособие / В.В. Паневчик, В.В. Акулич, С.В. Некраха, - Минск: БГЭУ,2012. – Ч.2. – 335с.

3. Паневчик В.В. Документационное и оргтехническое обеспечение управления: учеб. пособие / В.В. Паневчик, В.В. Акулич, С.В. Некраха / под ред. В.В.Паневчика.- Минск:БГЭУ,2008. – 318с.