Новый Перечень типовых управленческих архивных документов со сроками хранения

Из Министерства культуры пришла долгожданная новость: 8 сентября 2010 года Минюст зарегистрировал, наконец, «Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный приказом Минкультуры РФ еще 25 августа 2010 г. за № 558.

Как пишет «Консультант+», «Перечень состоит из 12 разделов, включающих в себя, в частности, документы, отражающие распорядительные, организационные функции управления, функции контроля; последовательно раскрывающие планирование, ценообразование, финансирование, учет и отчетность; об организации и осуществлении экономических, научно-технических, культурных и иных связей организаций; по организации труда; о работе с кадрами; о материально-техническом обеспечении и организации хранения имущественно-материальных ценностей; по административному и хозяйственному обслуживанию организаций; по социально-бытовым вопросам; по организации деятельности первичных профсоюзных и иных общественных организаций. В Перечне указаны сроки хранения документов на бумажных и электронных носителях, исчисление которых производится с 1 января года, следующего за годом окончания их делопроизводством».

Об этом Перечне мы еще не раз поговорим на страницах ближайших номеров журнала. И на нашем семинаре «Установление сроков хранения документов» ему уделим должное внимание (поробности на 1 стр. сентябрьского номера журнала).

Кстати, будет интересно посмотреть, какие из многочисленных существенных замечаний, которые были высказаны в отношении проекта этого документа в ходе его публичного обсуждения на форуме «Архивы России», были учтены в итоговом документе. Предстоит также разобраться, кому нужно срочно бежать переделывать свои номенклатуры, а кому пока можно и подождать.

Как должны быть оформлены копии учредительных документов при открытии счета в банке

Достаточно часто государственные органы, перечисляя виды документов, которые должны быть им представлены по тому или иному поводу и разрешая представлять их копии, пишут в нормативных документах, что копии должны быть заверены «в установленном порядке», но не уточняют, как именно (а ведь возможны варианты!).

Вот и Банк России в своей Инструкции от 14.09.2006 № 28-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам)» использовал эту общую формулировку. Теперь же в своем письме от 13.07.2010 № 011-31-1/3482 «О представлении копий учредительных документов при открытии счета» Банк России разъяснил, как он сам понимает «установленный порядок». Отныне заверение документов может быть осуществлено несколькими способами, в частности:

- должностным лицом банка (иным уполномоченным банком лицом) (п.1.11.2.). В этом случае в банк нужно будет представить и оригиналы документов;
- клиентом – юридическим лицом, – при условии установления должностным лицом банка (иным уполномоченным банком лицом) соответствия копий оригиналам документов (п.1.11.1), т.е. опять же потребуется представление подлинников документов в банк.

Кроме того, в письме обращается внимание на то, что инструкция не предусматривает возможности заверения «копий с копий». Это относится, прежде всего, к копиям учредительных документов, которые были выданы налоговыми органами. Такие копии «не могут рассматриваться в качестве оригиналов документов». Однако они «являются копиями, заверенными в порядке, установленным законодательством Российской Федерации, и могут быть получены кредитной организацией и помещены в соответствующее юридическое дело клиента».

Помимо этого, ЦБ указал, что Инструкция (п.1.11) предусматривает возможность представления в банк для открытия банковского счета, счета по вкладу (депозиту) и оригиналов необходимых документов.

Новый надежный способ уничтожения электронных документов и данных

Предлагаем вашему вниманию статью «Уничтожение электронных документов» видного американского специалиста Джесси Вилкинса (Jesse Wilkins), которая была недавно опубликована на блогах ассоциации специалистов по управлению контентом AIIM (http://aiimcommunities.org/erm/blog/destroying-erm).

«Одним из поводов для беспокойства, часто упоминаемым в связи с электронными документами, является то, что кнопка «Удалить»... этого не делает. Вообще говоря, когда удаляется электронный документ или какой-либо информационный объект, то в одной или нескольких системах, предназначенных для поиска объектов, стираются указатели на этот объект. Сами данные, однако, остаются доступными при использовании инструментария судебной экспертизы до тех пор, пока фактические адреса хранения не будут перезаписаны новым содержимым. Есть несколько подходов к решению этой задачи, в зависимости от конкретного типа носителя информации.

Для вращающихся жестких магнитных дисков, американский Национальный институт науки и технологии (NIST) признает три способа навсегда избавиться от контента. Первый – разрушить физическое устройство, распылив его на 5-мм частицы. Второй способ состоит в размагничивании диска в очень сильном магнитном поле. После такой обработки исчезает намагниченность пластин диска (и, следовательно, данные, хранящиеся на диске), но при этом часто также уничтожается и фирменная «прошивка» привода *(т.е. диск можно выбрасывать – Н.Х.)*. Жесткие диски типа ATA, изготовленные после 2001 года, могут быть очищены от содержащейся на них информации без разрушения диска с использованием специальной команды «защищенного стирания» (Secure Erase), которая полностью стирает каждый блок жесткого диска.

Это все хорошо и здорово для перезаписываемых носителей, но как быть с CD, DVD и другими WORM-носителями однократной записи? До недавних пор организации должны были либо записывать на каждый WORM-носитель документы одного срока хранения, и надеяться, на то, что часто применяемые в американской практике временные запреты на уничтожение документов в связи с судебными разбирательствами или расследованиями (legal hold) будут относиться ко всей информации на носителе, а не к какой то ее части, либо им приходилось использовать трудоемкий процесс миграции, в ходе которого, прежде, чем уничтожить первоначальный носитель информации, документы с более длительными сроками хранения переписывались с него на новый носитель. Это дорогостоящий, трудозатратный и подверженный ошибкам процесс – и горе той организации, которая сохранит документы годичного срока хранения и уничтожит документы с 10-летним сроком хранения, а не наоборот, как планировалось!

Но, возможно, есть иной путь. Несколько поставщиков разработали технологию, которую порой называют «цифровым шредированием» (digital shredding). 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 пульвериза-

ции. Это даже почти аналогично размагничиванию лент перед повторным использованием. Если размагничивание провести как надо, то очень 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.

Я считаю, что метод цифрового шредирования является на сегодня наиболее подходящим для обеспечения уничтожения электронных документов без излишнего бремени для организаций. Я не юрист, и не изображаю юриста на отраслевых конференциях. Однако думаю, что это хороший повод разобраться, как лучше всего применять наши испытанные и проверенные процедуры и практики по-новому, и так, чтоб их можно было защитить в суде.

Думаю, что мы просто обязаны разобраться в этом новом подходе и рекомендовать его нашим организациям; мы должны выявить его слабости и пути их преодоления, и включить его в состав наилучшей практики – точно так же, как мы поступали в прошлом в отношении методов уничтожения бумаги, магнитной ленты, микропленки, компакт-дисков и т.д. Это также означает включение упоминаний о нем в руководства, такие, как, скажем, стандарты DoD 5015.2 и MoReq, а также подталкивание сообщества поставщиков систем управления электронными документами и систем управления контентом разработать/лицензировать варианты этого метода и включить их в свои решения».

Новости подготовлены Натальей Храмцовской,
ведущим экспертом по управлению документацией компании «ЭОС»,
членом Гильдии Управляющих Документацией и ARMA International