Н.А. Храмцовская,
ведущий эксперт по управлению документацией компании «ЭОС»,
член Гильдии Управляющих Документацией и ARMA International

РАБОТА С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ В ВОПРОСАХ – ОТВЕТАХ

По каждому из приведенных ниже вопросов можно было бы написать диссертацию или выполнить консультационный проект, т. к. возможные решения зависят от особенностей работы конкретной организации, кроме того, будут в ближайшие годы меняться по мере перехода государственного управления на использование электронных документов. Поэтому ответы на вопросы даны лишь в общих чертах, без учета многочисленных особых ситуаций.

При работе с электронными документами следует помнить общее правило: по этим вопросам законодательно-нормативная база или устарела, или отсутствует, или, в лучшем случае, неполна. Поэтому организациям придется пока действовать на свой страх и риск. Высказанные ниже соображения во многом являются личной точкой зрения автора, поэтому использовать их следует только после дополнительной консультации с юристами предприятия.

Электронный документ – это:
- **документ, подписанный электронной подписью;**
- **скан-копия документа (например, исходящего письма)?**

В российском законодательстве определение понятия «электронный документ» дано в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 06.04.2011). Кроме того, ранее определение этого понятия приводилось в Федеральном законе от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» (в ред. от 08.11.2007), который перестал действовать с 01.07.2012.

Извлечение
из Федерального закона «Об информации, информационных технологиях и о защите информации»

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

[…]

11.1) электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

[…]

Извлечение
из Федерального закона «Об электронной цифровой подписи»

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

[…]
электронный документ – документ, в котором информация представлена в электронно-цифровой форме;
[…]

Кроме того, сейчас планируется внести изменения в ст. 434 Гражданского кодекса Российской Федерации, уточняющие понятие электронного документа:

Извлечение
из проекта Федерального закона № 47538-6
«О внесении изменений в части первую, вторую, третью и четвертую Гражданского кодекса Российской Федерации, а также в отдельные законодательные акты Российской Федерации»

224) в статье 434:
а) в пункте 2:
[…] дополнить абзацем вторым следующего содержания:
«Электронным документом, передаваемым по каналам связи, признается информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, магнитных, оптических или аналогичных средств, включая электронный обмен данными и электронную почту.»;
[…]

Хочу подчеркнуть, что главное качество электронного документа – то, что это документ; а его «электронность» является вторичным по важности свойством. На электронные документы в полной мере распространяются все требования законодательства, установленные для документов в целом.

В России незаверенная скан-копия является простой копией, не имеющей юридической силы, и, таким образом, документом не является.

Заверенная надлежащим образом скан-копия является документом, обычно имеющим ту же юридическую силу, что и заверенная бумажная копия. Надлежащим заверением, где этому не препятствуют требования действующего законодательства, в зависимости от конкретных обстоятельств (кто, что и с какой целью заверяет) будет ЭЦП, усиленная ЭП, квалифицированная ЭП либо ЭП нотариуса.

Приведем пример из арбитражной практики. При рассмотрении вопроса о правомочности признания общества уклонившимся от заключения контракта суды всех трех инстанций признали факт направления ООО «Энергия» оператору электронной площадки проекта контракта, подписанного электронной цифровой подписью, а также документа об обеспечении исполнения контракта (отсканированной копии проекта договора поручительства с приложенными отсканированными (сфотографированными) копиями документов на поручителя), подписанного электронной цифровой подписью, как доказательство исполнения обществом требований Федерального закона от 21.07.2005 № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» (в ред. от 12.12.2011) (Постановление ФАС Волго-Вятского округа от 15.02.2012 по делу № А28-4842/2011).

По истечении времени кто и как может подтвердить подлинность электронной подписи?

В настоящее время в законодательстве дано несколько определений различных видов электронных подписей.

Извлечение
из Федерального закона от 10.01.2002
№ 1-ФЗ «Об электронной цифровой подписи»[1]
(в ред. от 08.11.2007)

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

[…]
электронная цифровая подпись[2] – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;
[…]

Извлечение
из Федерального закона от 06.04.2011
№ 63-ФЗ «Об электронной цифровой подписи»
(в ред. от 01.07.2011)

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

[…]
1) **электронная подпись**[3] – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;
[…]

[1]Напоминаем, что указанный Федеральный закон прекратил свое действие с 01.07.2012.

[2]Выделено автором.

[3]Здесь и далее выделено автором.

Статья 5. Виды электронных подписей

[…]

2. **Простой электронной подписью** является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

3. **Неквалифицированной электронной подписью** является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

4. **Квалифицированной электронной подписью** является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

[…]

Вопрос о подтверждении подлинности электронной подписи прежде всего связан с теми ее видами, которые создаются в результате криптографического преобразования информации с использованием закрытого ключа/ключа подписания (это ЭЦП, усиленные неквалифицированная и квалифицированная электронные подписи).

Если надлежащим образом задокументировано время создания (получения) документа, то, пока существует удостоверяющий центр, выдавший сертификат подписи (далее – УЦ), подлинность подписи обычно может быть подтверждена им с использованием специального программного обеспечения. Процедура такой проверки в обязательном порядке устанавливается договором об использовании услуг УЦ или о присоединении к корпоративной системе электронного документооборота. Если УЦ прекратил свою деятельность, а его документация не была в полном объеме передана в другой УЦ, возможны серьезные проблемы.

Следует иметь в виду, что в настоящее время для «исторических» подписей может быть затруднительно доказать время подписания (особенно если документ не был зарегистрирован, например, в СЭД). Невозможность доказать для «исторической» подписи время подписания делает невозможным подтверждение подлинности документа.

В общем случае отсутствуют также правовые основания для использования механизмов отметок времени, переподписания документа новой удостоверяющей подписью или «снятия» ЭЦП при передаче документа на архивное хранение, используемых за рубежом. У нас такие механизмы в настоящее время могут использоваться только в корпоративных системах по соглашению сторон.

Именно по этой причине пока не рекомендуется использовать ЭЦП или усиленные подписи для подписания документов длительного и постоянного хранения. Иногда проблема длительного хранения решается тем, что вместе с электронным документом, подписанным ЭЦП, создается бумажный дубликат с «мокрой» подписью и печатью, который и уходит на архивное хранение.

Как хранить электронные документы на предприятии:

- **на сервере;**
- **в виде резервных копий[4];**
- **на отчуждаемых машинных носителях?**

Каковы особенности каждого вида хранения и их процедурные отличия?

Правильное сочетание технических, нормативно-правовых и организационных мер обеспечивает надлежащее хранение документов по любой технологии, кроме использования резервных копий информационных систем. Здесь есть правовая проблема: в настоящее время только начинают появляться отечественные нормативные требования к хранению электронных документов, и впереди организации могут ждать неприятные сюрпризы.

Указание Банка России от 25.11.2009 № 2346-У «О хранении в кредитной организации в электронном виде отдельных документов, связанных с оформлением бухгалтерских, расчетных и кассовых операций при организации работ по ведению бухгалтерского учета» стало первым нормативным документом в нашей стране, в котором были установлены конкретные требования регулятора к организации хранения электронных документов. В нем Банк России предписывает хранить первичные документы бухгалтерского учета только на оптических носителях однократной записи. Если ФНС России или какой-либо другой контролирующий орган установит собственные, отличающиеся требования к хранению электронных документов (например, в виде электронных баз данных), то кредитным организациям придется вести два совершенно разных электронных архива, что может быть весьма неудобно и накладно.

По сути дела, действующее законодательство пока позволяет хранить документы, подписанные ЭЦП (усиленной подписью), любым способом, – но все хорошо до тех пор, пока сохраняется возможность перепроверить ЭЦП. Исключением являются государственные реестры и регистры, эксплуатация которых регулируется отдельно.

Существует ряд международных стандартов, содержащих рекомендации по хранению электронных документов. Некоторые из них переведены или переводятся на русский язык.

С 2010 г. подкомитет ПК 6 «Жизненный цикл электронного документооборота» (в составе технического

[4]Резервное копирование (англ. backup) – процесс создания копии данных на носителе (жестком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

комитета Росстандарта ТК459), созданный на базе компании «Электронные офисные системы», ведет работы по переводу и адаптации в качестве российских стандартов ряда стандартов Международной организации по стандартизации (ИСО), посвященных вопросам обеспечения сохранности электронных документов.

В ближайшее время должен быть опубликован ГОСТ Р 54471-2011/ISO/TR 15801:2009 «Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности». Данный стандарт описывает средства, с помощью которых в любой момент может быть продемонстрировано, что содержание (контент) конкретного электронного объекта, созданного или существующего в рамках компьютерной системы, не изменилось с момента его создания в системе либо с момента импорта в нее.

В 2012 г. планируется утверждение ГОСТ Р/ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов». Этот стандарт является обобщением многолетнего передового мирового опыта по обеспечению долговременной сохранности не просто информации, а юридически значимых электронных документов, в т. ч. и в случае проведения их конверсии/миграции на другие носители и в другие форматы и системы. Следование содержащимся в стандарте рекомендациям существенно повышает вероятность успешного сохранения юридически значимых документов, хотя, безусловно, достижение этой цели возможно только при условии исполнения законодательно-нормативных требований к хранению электронных документов, которые в России только-только начали появляться.

Кто несет ответственность за хранение электронных документов?

Ответственность за хранение документов несут организация и ее руководитель (именно их будут штрафовать). Руководитель организации, если он сочтет нужным, вправе делегировать эту ответственность отдельным подразделениям и специалистам.

Как осуществляется перезапись электронных документов в случае хранения в архиве и миграция данных в случае хранения на сервере?

Если информация хранится на носителях, то их читаемость должна регулярно контролироваться, и при первых признаках проблем их следует перезаписывать. Можно найти рекомендации, как это делать, в т. ч. в соответствующих указаниях Банка России (которые, правда, с моей точки зрения, содержат ряд ошибок).

По мере устаревания носителей, форматов, оборудования, программного обеспечения информацию следует переносить и/или преобразовывать, обязательно сохраняя подлинники. Существуют международные стандарты, содержащие рекомендации по проведению конверсии и миграции.

Как внести изменения в локальные нормативные акты предприятия в части передачи электронных документов на хранение в архив (в настоящее время электронные документы в архив не передаются, хранятся на сервере)?

Начать надо с общения с архивом. Скорее всего, вам предложат в обозримом будущем продолжить хранение электронных документов у себя. Выясните требования архива, чтобы потом к вам не было претензий. После этого желательно изучить мировую практику хранения электронных документов и, пока не появятся отечественные нормативные требования, следовать ей.

Рекомендую использовать подход, аналогичный системе менеджмента качества: вы определяете не противоречащий законодательству и требованиям архива порядок хранения, выпускаете внутренний нормативный документ, действуете строго в соответствии с ними и собираете на каждом этапе документы, доказывающие, что все делается как надо.

Каков механизм доступа к электронным документам в случае их хранения на сервере, а не в архиве?

При хранении на сервере вы используете те меры защиты и управления доступом, которые у вас есть, подкрепляя их организационными мерами, определяющими порядок доступа, права и ответственность и т. д.

Обязательно нужно иметь несколько страховых и резервных копий, сохраняя как минимум один комплект копий в территориально удаленном хранилище.

Как уничтожаются электронные документы в случае их хранения на сервере, а не в архиве?

При уничтожении следует постараться уничтожить все копии. Что касается копий информации, содержащихся в резервных копиях, то желательно продумать процедуру регулярной перезаписи таких копий, чтобы через разумное время на них уже не оставалось удаленной в «боевой» системе информации. Информацию можно считать по-настоящему удаленной только тогда, когда ее больше нет в т. ч. и в виде резервных копий.

Удобнее, чтобы уничтожение инициировал и окончательно оформлял архив, а большинство остальных операций выполняла IT-служба.

Какую информацию должен содержать акт об уничтожении электронных документов?

Законодательство не обязывает организацию включать в акт больше сведений, чем при уничтожении бумажных документов.

Акт об уничтожении в том виде, в каком он приведен в Приложении 4 к Основным Правилам работы архивов организаций (одобрены решением Коллегии Росархива от 06.02.2002, нормативным документом не являются)

и в Приложении 3 к Основным правилам работы ведомственных архивов (утверждены приказом Главархива СССР от 05.09.1985 № 263), содержит:

- сведения о нормативных документах, на основе которых документы отбирались к уничтожению;
- заголовки дел или групповые заголовки документов, крайние даты, индексы по номенклатуре или номера по описи, количество единиц хранения, сроки хранения и соответствующие нормативные ссылки;
- сведения о том, кем, когда, в каком количестве и каким методом документы уничтожались.

Фактически требуется идентифицировать уничтожаемые документы с точностью, позволяющей экспертной комиссии установить сроки их хранения, условия отсчета этих сроков и убедиться в истечении сроков хранения. Опыт коммерческих организаций и судебная практика показывают, что даже в традиционном делопроизводстве описание уничтожаемых документов на уровне групп или дел нередко является недостаточным как для экспертной комиссии, так и в случае судебных споров, и иногда желательно более детальное описание (например, отдельно по каждому контрагенту, тендеру, договору и т. д.).

Особенностью электронных документов является наличие многочисленных дубликатов. С моей точки зрения, желательно позаботиться о максимально полном их уничтожении, особенно в составе резервных копий, и отметить соответствующие факты в акте.

Что является результатом уничтожения электронного документа:

- **невозможность воспроизведения:**
  – документа и его регистрационно-контрольной карточки (РКК);
  – только документа, когда РКК остается в качестве справочного аппарата и содержит пометку о состоянии документа «уничтожен»;
- **отсутствие доступа к тому/делу;**
- **другое?**

Как правило, результатом уничтожения документа является необратимое уничтожение его содержания, а также большинства его метаданных (реквизитов), так, чтобы не было возможности (с использованием разумных усилий) восстановить эту информацию.

Законодательство не требует сохранять реквизиты, даже основные, всех уничтоженных документов (достаточно сохранить сведения на уровне дел/групп документов – см. содержание акта об уничтожении), и здесь организация должна исходить из существующих в отношении конкретных видов документов законодательно-нормативных требований, потребности в доказывании факта того, что конкретные документы существовали, но были уничтожены (например, исходя из судебной практики), степени секретности (конфиденциальности) сведений и возможности их раскрытия через сохраненные реквизиты, собственных потребностей в информации и т. д.

Отсутствие доступа не может считаться надлежащим уничтожением, равно как и применение любого иного метода, не обеспечивающего невозможность восстановления информации.

Рекомендую почитать раздел 5 спецификации MoReq2 (перевод на русский язык) (http://www.dlmforum.eu/index.php?option=com_jotloader&section=files&task=download&cid=189_dcd3aff30cbc4ea4a5ad84e2daaeca20&Itemid=39&lang=en).

Кто должен производить уничтожение – специалисты архива предприятия или IT-отдела?

Каких-либо законодательных требований, регламентирующих данный вопрос, мне не известно. Организация может и должна разработать свой собственный порядок уничтожения электронных документов и зафиксировать его в виде внутреннего нормативного документа.

Если документы уничтожаются путем физического уничтожения носителей, то данный процесс принципиально не отличается от физического уничтожения бумажных дел и нередко может быть поручен тому же подразделению.

Если документы уничтожаются путем стирания или перезаписи, то соответствующую операцию должен проводить специально обученный сотрудник, имеющий (если стирание проводится в информационной системе) надлежащую авторизацию, под наблюдением члена (членов) экспертной комиссии. Надежнее, если специалист архива и IT-специалист будут делать это совместно.

Некоторые действия, связанные с уничтожением электронных документов, не требуют непосредственного участия представителя архива (например, размагничивание носителя информации, перезапись резервных копий) и могут выполняться IT-подразделением самостоятельно.

Как следует формировать электронные тома (дела), электронно-бумажные тома (дела)? Могут ли в один том (дело) формироваться бумажные документы (подлинники) электронных документов, подписанные электронной подписью, и скан-образы документов?

В условиях смешанного документооборота может получиться так, что одни документы, входящие в состав дела, будут электронными, а другие – бумажными. Физически хранить их вместе иногда возможно (например, вкладывая CD или DVD в бумажное дело), но данный подход чреват большими проблемами при длительном хранении.

Наиболее распространенной в мире практикой является единый учет всех документов, вне зависимости от вида носителя (например, в СЭД). Обратите внимание на то, что с точки зрения учета и доступа электронные документы на съемных носителях могут быть куда ближе к бумажным документам, чем к электронным документам, хранящимся в СЭД.

Когда дело состоит из электронной и бумажной частей, очень желательно (но не обязательно) одну из этих частей дополнить копиями, чтобы был полный комплект.

С точки зрения удобства оперативной работы с информацией, как правило, лучше дополнить электронными образами бумажных документов электронную часть дела.

Помещение в одно (например, электронное) дело подлинников и заверенных и незаверенных копий вполне допустимо, однако следует позаботиться о том, чтобы в тех случаях, когда пользователь работает с копией, было ясно, что это не подлинник, чтобы был понятен статус копии (заверенная, незаверенная) и есть ли в организации оригинал (и если есть, то где хранится). Аналогичным образом в бумажной части дела желательно указывать на существование и место хранения электронной части.

Изредка, но встречаются организации с настолько хорошей дисциплиной делопроизводства, что они раздельно, без копирования учитывают и хранят электронную и бумажную части дел и обеспечивают неразрывную связь между ними за счет организационных мер.

Что указывается в описи дел постоянного хранения? Подсчитывать ли количество томов с электронными документами?

Если ваша организация – источник комплектования архива, то этот вопрос следует задать архиву.

Если тома электронных документов реально существуют, указывайте их. Если тома на самом деле не формируются, указывайте количество документов или, где это уместно, носителей документов (например, оптических носителей однократной записи).

В какой государственный архив передавать документы и в каком виде? Как определить формат передачи электронных документов в государственный архив?

Если ваша организация – источник комплектования архива, то этот вопрос следует задать архиву. При этом будьте готовы к тому, что не получите внятного ответа.

Сейчас планируется создать государственный электронный архив, но этот проект пока находится в зачаточном состоянии. С моей точки зрения, в настоящее время ни один государственный архив не способен обеспечить длительное хранение электронных документов, так что даже если их у вас и примут, оставьте у себя дубликаты и готовьтесь впоследствии передавать эти документы повторно.

Как минимум вы должны передать в архив подлинники, т. е. документы в их исходном формате. Я предложила бы вам также подумать (там, где вы сами в этом заинтересованы) об изготовлении заверенных копий в форматах, которые в мире считаются наиболее подходящими для длительного хранения документов (например, PDF/A, некоторые версии TIFF и т. п.).

Вопрос о передаче метаданных документов архивы вряд ли готовы обсуждать, какого-то единого стандарта здесь нет, и не думаю, что он вскоре появится. Однако хорошо, если у вас будет возможность выдавать метаданные документов из всех информационных систем вашей организации в каком-то одном формате, каким бы он ни был.

При учете электронных копий документов в номенклатуре дел, томе (деле) нужно ли учитывать электронные копии документов (например, электронный документ направлен на исполнение ответственному исполнителю и соисполнителям)?

Как и в бумажном делопроизводстве, учет копий следует вести в тех случаях, когда это оправдывается интересами деловой деятельности и обеспечения информационной безопасности (например, для полноты последующего уничтожения). С точки зрения ответственного исполнителя получаемые им копии могут быть важным документом, подтверждающим его деятельность, и если он их регулярно сохраняет в отдельном месте, то их следует включать в номенклатуру.

Если документы хранятся в электронном виде, то как их указать в итоговой записи к номенклатуре дел? Что считать единицей учета?

Если ваша организация – источник комплектования архива, то начните с того, что задайте такого рода вопросы архиву. Архивы часто крайне консервативны и не склонны менять свои привычки, даже если изменилась законодательно-нормативная база.

Здесь рекомендую исходить из имеющихся у вас возможностей. Например, если СЭД организации позволяет тем или иным способом формировать электронные дела, то можно указать количество таких дел. Если же нет, можно указать число документов.

При использовании съемных носителей (если только не смешивать на одном носителе документы разных видов) в ряде случаев можно учитывать количество носителей.

Выбранный подход желательно закрепить во внутреннем нормативном документе организации.

При проведении экспертизы ценности электронных документов нужны ли специальные отметки в протоколе заседания ЭК? Если да – какого рода они должны быть?

Общий принцип следующий: срок хранения документов определяется их содержанием и не зависит от вида носителя.

В то же время возможны исключения, когда, например, массив электронной информации, снабженный хорошей машиной поиска, имеет намного большую ценность, чем та же информация на бумаге. Кроме того, форма и место хранения информации могут иметь значение для выбора процедуры уничтожения. Поэтому там, где форма и место хранения не очевидны по умолчанию, думаю, стоит их указывать. ■