



ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо довгострокового зберігання інформаційних ресурсів.

У публікації «Гибридный подход в обеспечении сохранности и доступности документов» висвітлено створення гібридних систем та пропонуються шляхи використання оцифрованої інформації.

У публікації «Как решать проблему длительного хранения документов с учетом устаревания форматов и носителей?» проаналізовано стан та надано рекомендації щодо роботи з електронними документами.

У публікації «Проблемы и перспективы облаков: мнение читателей PC Week, комментарии экспертов» наведено проблеми та перспективи використання хмарних технологій.

У публікації «HP helion continuity services: аварийное восстановление как сервис» розповідається про сервіс HP Helion для аварійного відновлення.

У публікації «Управление электронной почтой в государственных органах Великобритании – комментарии государственного служащего» розповідається про недоліки в управлінні електронною поштою в державних органах Великобританії.

У публікації «Практика хранения документов с электронной подписью» розповідається, як вирішується принципове завдання архівного зберігання електронного документа - забезпечення юридичної значимості документа, термін зберігання якого перевищує термін дії сертифіката електронного підпису.

У публікації «На сайте Британского института стандартов начато публичное обсуждение проекта новой редакции стандарта ISO/IEC 27000 «Системы менеджмента информационной безопасности. Общий обзор и терминология» надано інформацію про обговорення проекту стандарту ISO/IEC 27000.

У публікації «Пионер Интернета предупреждает о том, что наша эпоха может стать «электронными темными веками»» розповідається про можливі проблеми з використанням сучасних електронних документів.

У публікації «Большие данные: Оставляя позади неудачный опыт первых внедрений» розповідається про проблеми та подальші перспективи використання Великих даних.

У публікації «Требования к порядку межведомственного информационного взаимодействия при предоставлении государственных и муниципальных услуг и исполнении функций в электронной форме» інформується про затвердження вимог щодо порядку міжвідомчої інформаційної взаємодії під час надання державних та муніципальних послуг.

У публікації «Австралийский опыт проведения самооценки электронного хранилища учреждения на соответствие требованиям к доверенным хранилищам стандарта ISO 16363-2012» надано оцінку стандарту ISO 16363, описано процес самооцінки та наведено рекомендації для всіх тих, хто хотів би здійснити аналогічні проекти.

У публікації «США: Шум по поводу электронной переписки Хиллари Клинтон и скрытая за ним скандальная проблема» розповідається, що Хілларі Клінтон, під час перебування на посту державного секретаря, в порушення законодавства вела свою електронну переписку не через підконтрольний державі поштовий сервер, а через власний, в результаті чого потенційно могли бути знищені державні документи що підлягають постійному зберіганню і допущений витік секретної інформації.

У публікації «Национальные Архивы США используют решение «Единый архив» компании ZL Technologies для управления неструктурированными данными» розповідається про розробку компанією «ZL Technologies» рішення ZL UA що не має собі рівних в плані масштабованості і підтримки детального управління і контролю над неструктурованим контентом.

У публікації «Когда (не) нужно мигрировать с формата PDF на PDF/A» розповідається про переваги та недоліки міграції.

У публікації «Дания: Открылся крупнейший цифровой архив страны» розповідається про відкриття найбільшого цифрового архіву країни.



ГИБРИДНЫЙ ПОДХОД В ОБЕСПЕЧЕНИИ СОХРАННОСТИ И ДОСТУПНОСТИ ДОКУМЕНТОВ

Источник:

Авторы: Дубинин С. С. Репроникс Лтд., Тула, Россия

Кисловская Г. А. ВГБИЛ им. М. И. Рудомино, Москва, Россия

Настоящий доклад посвящен вопросам применения гибридного подхода (микрофильмирование и оцифровывание) для целей обеспечения сохранности и доступности документов. Доклад содержит результаты экспериментальных работ по созданию гибридных систем, требования к параметрам сканирования и предлагает пути дальнейшего использования оцифрованной информации.

Информация, заключающая в себе мировой опыт человечества, служащая исторической памятью и основой дальнейшего экономического и духовного прогресса общества, хранится в библиотеках и архивах мира, как правило, в виде бумажных документов.

Глобальной задачей является сохранение для грядущих поколений этой бесценной информации, ее носителей и обеспечение доступности к ней.

В мировой практике различают два подхода к обеспечению сохранности документов:

- сохранность собственно документа (носителя информации);
- сохранность интеллектуального содержания документа.

Первый подход обеспечивается применением консервативных мер. Второй — использованием технологий переформатирования, т. е. перевода информации с одного носителя информации на другой, более долговечный.

Переформатирование документов является экономичной и эффективной мерой. В отличие от дорогостоящих мер по консервации и реставрации перенос информации на другие носители обеспечивает существенное расширение доступа к сохраняемым документам.

Наиболее распространенной технологией переформатирования является микрофильмирование.

Микрофильм, изготовленный на галогенидосеребряной пленке в соответствии с международными стандартами и хранящийся в специальных условиях, обеспечивает сохранность информации, по некоторым данным, до 500 и даже 1000 лет.

Технология микрофильмирования консервативна, т. е. в ней не происходят существенные преобразования. Хранимая информация доступна, с относительно небольшим усилием, человеческому глазу. Развитая система стандартизации гарантирует совместное использование микрофильмов во всем мире.

Микрофильм м. б. создан с относительно небольшими затратами, объединен с системами автоматизированного доступа, переведен в цифровую форму.

Развитие цифровых технологий дало возможность повысить удобство и оперативность использования информации хранимой на документах путем перевода ее в цифровую форму для дальнейшего использования в вычислительных системах и сетях, что обеспечивает возможность удаленного доступа, дальнейшую обработку и существенно расширяет круг пользователей.

Такой гибридный подход (когда для обеспечения сохранности документов используется микрофильм, а для поиска, обработки и т. д. — средства вычислительной техники) к построению систем обеспечения сохранности и доступности документов позволяет в настоящее время создавать эффективные многоуровневые системы хранения и использования документов.

Каковы возможные подходы в обеспечении сохранности и доступности документов с использованием “гибридных технологий”?

Здесь можно выделить два этапа:

1. Микрофильмирование документов для обеспечения сохранности

Цель — создать страховой фонд документации, являющейся национальным научным, культурным и историческим наследием.

В соответствии с разработанным государственным стандартом РФ “ЕР СФД. Порядок создания страхового фонда документации, являющейся национальным научным, культурным и историческим наследием” должны быть изготовлены:

— негативная микроформа первого поколения (страховая копия документа) на черно-белой фотографической галогенидосеребряной пленке, методом непосредственного фотографирования документа;

Одновременно с созданием страхового фонда изготавливается комплект пользовательских копий (фонд пользования), включающий:

— микрофильм второго поколения на галогенидосеребряной пленке изготавливаемый со страховой копии (основная копия фонда пользования);

— рабочую копию (3-е поколение), изготовленную с основной копии фонда пользования.

Страховые копии должны быть переданы на хранение в специальное хранилище территориально обособленное от оригиналов документов.

Микроформы страхового фонда изготавливаются в виде рулонного микрофильма МР-35 или микрофиш типоразмера МФ-А6.

Микрофильмы фонда пользования используются для последующего получения копий (в т. ч. и в цифровой форме) и обслуживания читателей.

2. Создание подсистемы обеспечения доступности к хранимой информации

Здесь возможны следующие подходы:

2. 1. Использование существующих карточных (или автоматизированных) каталогов, в которые добавляется адрес хранения документа на микрофильме.

2. 2. Создание специализированной автоматизированной информационно-поисковой системы (АИПС), содержащей библиографическое описание документа, аннотацию (ключевые слова) и/или специальный рубрикатор.

В этом случае поиск необходимого документа производится на основании библиографических полей описания документа, ключевых слов и логических операторов (и, или, не и др.). Результатом поиска является адрес хранения документа на микрофильме.

Доступ к микрофильму в этом случае может быть осуществлен:

— ручным способом (адрес: шкаф, полка, ячейка; установить микрофильм в читальный (читально-копировальный) аппарат, найти требуемый кадр, просмотреть и получить копию в случае необходимости);

— автоматизированным способом (адрес: шкаф, полка, ячейка; установить микрофильм (кассету с микрофишами) в читальный аппарат с автоматизированным поиском и используя клавиатуру аппарата (или непосредственное управление от ЭВМ) выбрать и установить на экране требуемый кадр);

— автоматическим способом (непосредственное управление автоматизированным хранилищем от ЭВМ).

Это так называемые незаслуженно забытые в настоящее время CAR-системы. В 80 — начало 90-х годов нами была создана гамма систем, ориентированных на использование различных видов документации (конструкторской, технологической, нормативно-технической, патентной, научно-технической, медицинской, юридической и др.).

2. 3. Недостатком CAR-систем являлась ручная обработка исходных данных для подготовки описания документа (в первую очередь составление аннотации документа). Аннотацию готовил один человек (и не всегда специалист в данной отрасли), поиск производил другой человек (и не всегда они говорили на одном языке). Результатом являлся “большой информационный шум” и невысокий уровень релевантности запросов к системе.

Развитие средств ВТ и, в первую очередь, систем распознавания текста (OCR-систем) позволяют в достаточной степени устранить указанные недостатки.

Система доступа в этом случае может быть построена по следующему принципу:

— проводится сканирование микрофильма;

— перевод его в текстовую форму (автоматическое распознавание) и формирование полнотекстовой базы данных;

— установление связей между фрагментами текста и графическим изображением информации, хранимой на кадре микрофильма.

Данный подход позволяет получить полнотекстовую базу данных (в автоматизированном режиме, без участия человека в исправлении ошибок), содержащую по нашим данным от 7 до 10% ошибок.

Поиск производится по ключевым словам с использованием операторов (И, ИЛИ, НЕ, маскирования окончания и др.).

Результатом поиска является распознанный текст, который можно просмотреть на экране ПК, данный текст связан с графическим изображением исходного фрагмента документа (включая сопутствующие рисунки, фотографии и др.) и всегда можно получить адрес хранения исходного документа на микрофильме.

Нами была разработана экспериментальная система на базе пакета прикладных программ “Евфрат-99”. Исходной информацией для наполнения полнотекстовой базы данных являлась газета “Московские новости”, 1981 г. Сканирование проводилось с микрофильма (3-е поколение) без участия человека в исправлении ошибок в процессе распознавания. Наличие ошибок практически не влияло на точность поиска, всегда можно было перейти к графическому изображению исходного документа (для целей экономии аппаратных средств использовался режим с разрешением 150 dpi.) или для получения более высококачественного изображения использовать микрофильм.

2. 4. Следующий подход, который может быть использован в доступе к информации.

Его можно назвать “цифровое копирование”. Проводится сканирование документа с микрофильма, перевод его в формат пакета Adobe Acrobat (PDF).

Перевод в формат PDF имеет ряд преимуществ:

— объем получаемых файлов примерно в 10 раз меньше, чем в формате TIFF;

— есть возможность устанавливать ссылки между фрагментами текста, включать различные приложения и т. д.;

— программная оболочка Acrobat Reader доступна практически всем, что не требует разработки отдельных программных приложений, и позволяет вести обмен информации между пользователями в одном формате.

Экспериментально были проведены работы по оцифровыванию изданий и перевод их в формат PDF. Исходная информация: Слащёв-Крымский. Требую суда общества и гласности (оборона и сдача Крыма). Константинополь, 1921 (из фондов ГПИБ, Москва). Исходный объем — 95 стр. Разрешение при сканировании 300 dpi. Полученный объем — 3, 8 Мб. По содержанию возможен доступ к любой главе, пролистывание вперед, назад, печать на принтере.

Отдельно хотелось бы коснуться вопросов, связанных с требованиями к параметрам оцифровывания информации с микрофильма или бумаги.

В соответствии со стандартом ISO 6199 для оценки качества изображения используется коэффициент (индекс) качества QI. Значение QI для низкого качества (3, 6), среднего (5, 0), высокого (8, 0). Сотрудниками лаборатории Корнельского университета была предложена формула для перевода значения коэффициента качества (QI) в оптическое разрешение при сканировании изображения.

Для черно-белого сканирования значение оптического разрешения получают:

- низкое качество (QI=3, 6) — 277 dpi;
- среднее качество (QI=5, 0) — 384 dpi;
- высокое качество (QI=8, 0) — 615 dpi.

Объективная оценка качества получаемого оцифрованного изображения является в определенном смысле проблемой, связанной с восприятием человеком графической информации.

Нами были проведены экспериментальные работы по оценке влияния параметров сканирования (оптическое разрешение, контрастность (порог чувствительности)) на качество получаемого оцифрованного изображения.

Для оценки качества использовалась программа оптического распознавания Fine Reader (оценивался получаемый % ошибок распознавания текста).

Для этого были подготовлены эталонные документы на бумаге, которые затем микрофильмировались и с обоих носителей проводилось оцифровывание информации. Результаты оцифровывания (с различными значениями параметров сканирования) сравнивались.

Результаты (для черно-белого сканирования):

- для документов хорошего качества следует использовать разрешение не менее 300 dpi., что соответствует QI = 3, 6;
- различия в распознавании текста с разрешениями 400 и 600 dpi. незначительны. Поэтому сканирование текстов с разрешением более 400 dpi. целесообразно лишь в случаях оцифровывания некачественных оригиналов или наличия мелких (менее 6 пунктов) символов (QI = 5, 0—8, 0);
- на качество оцифровывания в большей степени влияет параметр порога распознаваемости (контрастность). При неудачном выборе этого порога увеличение оптического разрешения не дает практического выигрыша, т. к. может быть полная потеря мелких деталей изображения или, наоборот, “заплывание” участков текста.

Оптимальный порог может варьировать от документа к документу. Например, тексты с использованием гарнитур “с засечками” (Таймс, Антикава) требуют более низких значений порога (10—15%), чем рубленые гарнитуры (Гельветика, Курьер).

Сочетание на одной странице документа текстов, набранных различными гарнитурами, что часто встречается в газетной и журнальной полиграфической продукции, значительно затрудняет определение оптимального порога распознавания.

Выводы:

1. Подходов к построению гибридных систем достаточно много.
2. Базовой основой для архивного хранения и оцифровывания должен являться (в обозримом будущем) микрофильм.

Преимущества:

- сканирование производится с носителя одного формата (например, 35-мм пленки), что значительно снижает издержки;
- в процессе проведения микрофильмирования иногда удается улучшить качество изображения (устранение нежелательного фона, увеличения контрастности и т. д.);
- в связи с тем, что проводятся работы по созданию страхового микрофильма, осуществляется устранение лагун в издании, реставрация издания и т. д.

3. Системы обеспечения сохранности и доступности документов должны быть многоуровневыми. Перевод информации в цифровую форму необходим для достижения определенных целей (например: дальнейшая компьютерная обработка, активный оперативный доступ и т. д.).



КАК РЕШАТЬ ПРОБЛЕМУ ДЛИТЕЛЬНОГО ХРАНЕНИЯ ДОКУМЕНТОВ С УЧЕТОМ УСТАРЕВАНИЯ ФОРМАТОВ И НОСИТЕЛЕЙ?

Источник: <http://ecm-journal.ru/post/Kak-reshat-problemu-dlitelnogo-khranenija-dokumentov-s-uchetom-ustarevanija-formatov-i-nositelej.aspx>

Автор: Павел Овчинников



Вопрос читателя: Как решить проблему длительного хранения документов с учетом устаревания форматов и носителей?

Ответ:

Действительно, состояние физических носителей вызывает ряд сомнений. На сегодняшний день вечных вариантов хранения цифровых данных практически нет: магнитные диски размагничиваются со временем, полупроводниковые накопители теряют заряд, а оптические диски, записанные в обычных условиях, тоже приходят в негодность. Мы пока не

сталкивались с проблемой носителей, ведь история электронных документов еще слишком коротка. А пока компаниям придется тщательно планировать хранение: обеспечивать резервное копирование и мониторинг.

Что касается форматов, то тут ситуация аналогичная. Следует помнить, что форматы хранения данных тоже устаревают и надо выбирать тот вариант, который теоретически может быть более долговечен. Сегодня важные документы преимущественно создаются в форматах, которые являются открытыми, то есть сохраняют возможность прочитать документ даже без приложения, в котором его создали изначально. Например, для текстовых документов это форматы .xml, .pdf, .txt и некоторые другие. Мы можем просмотреть эти файлы почти в любом современном редакторе.

Пока нет устоявшейся практики работы с электронными документами длительного срока хранения, мы можем только предлагать ряд рекомендаций:

- Во-первых, использовать в электронном виде документы, чьи сроки хранения не превышают 15 лет. Для остальных документов внимательно оценивать целесообразность их перевода в электронный вид, посчитать затраты на их длительное хранение в электронном виде.

- Во-вторых, использовать для документов общераспространённые открытые форматы документов, которые уже используются в течение нескольких лет.

- В-третьих, позаботиться заранее о резервном копировании и наличии устройств считывания тех носителей, на которых вы храните документы.

Думаю, что следуя этим рекомендациям, вы обеспечите себе минимальные гарантии хранения электронных документов.



ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЛАКОВ: МНЕНИЕ ЧИТАТЕЛЕЙ PC WEEK, КОММЕНТАРИИ ЭКСПЕРТОВ

Источник: <http://www.pcweek.ru/its/sap-cloud/2.php>

Когда речь заходит о реальном применении облачных решений в бизнесе, мы нередко наблюдаем крайнюю поляризацию мнений. Одни видят в облаках будущее и готовы идти в этом направлении уже сейчас, другие выражают крайний скепсис и отмечают серьезные проблемы (а они, несомненно, есть). Редакция PC Week попыталась прояснить картину, проведя опрос среди своих читателей.

Как нам кажется, выборка получилась достаточно репрезентативная. Около 62% респондентов представляют предприятия сегмента СМБ (37% с численностью до 100 сотрудников и 25% – от 100 до 500). Получили мы отклики и от весьма крупных компаний (со штатом более 5000), таковых оказалось 8%. Получают ли от крупных вендоров нынешние пользователи их продуктов предложения по развертыванию тех или иных решений в облаках?



Рис. 1 – Ответы на вопрос: Использует ли ваша компания какие-либо облачные SaaS- и/или PaaS-сервисы?

Довольно неожиданно оказалось, что 44% компаний подобных предложений вообще не поступало. Еще 18-ти процентам их предлагают в комплекте с дополнительными услугами по развертыванию и поддержке (собственными и партнерскими), 17-ти процентам предлагают, но на базе зарубежных ЦОДов и 15-ти процентам – через инфраструктуру своих партнеров.

Директор по продажам бизнес-приложений SAP СНГ Павел Растопшин сообщил, что его компания использует проактивный подход в работе с облачными заказчиками и регулярно общается по данной теме с ИТ-сообществом. Сейчас для клиентов SAP важны такие вопросы, как широта спектра бизнес-сценариев, которые можно использовать в облаке, модели расчета возврата от инвестиций и совокупной стоимости владения (ТСО) для разных вариантов развертывания (облачных или гибридных), примеры внедрений в России и за рубежом. Коммерческий директор «Эй Би Си Консалтинг» Михаил Энгельгардт добавляет, что у многих ИТ-служб отсутствует четкое понимание вопросов обеспечения безопасности данных, архитектуры интеграции и качественной оценки рисков использования облачных сервисов.

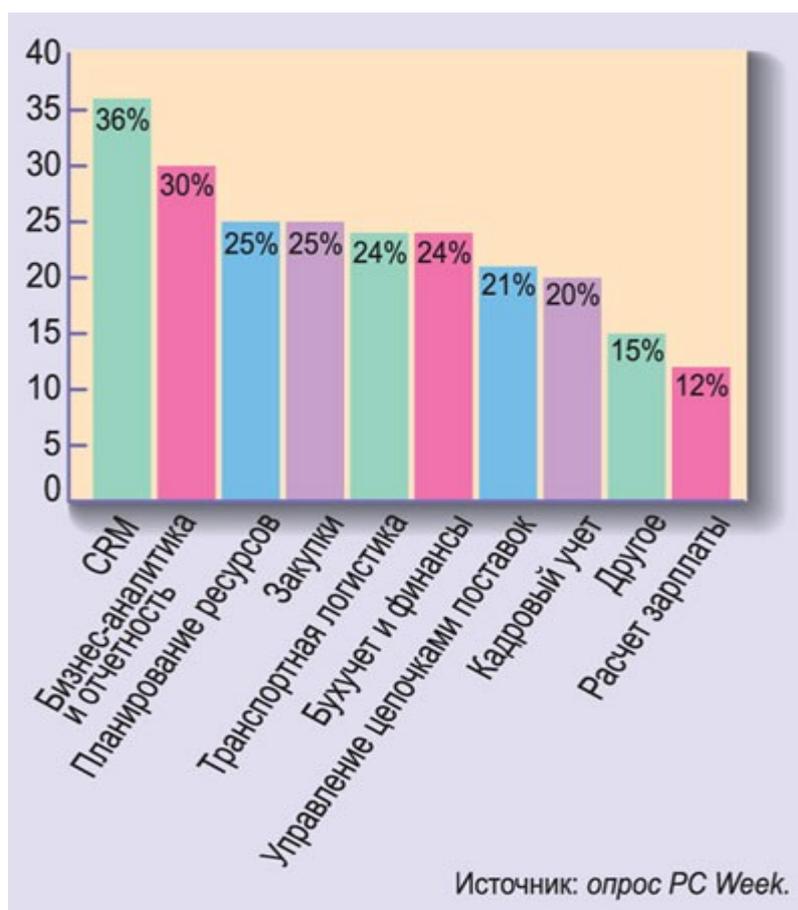


Рис. 2 – Ответы на вопрос: Какие функции корпоративного управления, с вашей точки зрения, целесообразно получать в виде облачной услуги?

А руководитель направления CRM компании itelligence Артем Третьяк объясняет недостаточную популярность облачных решений в России не столько дефицитом информации, сколько относительной новизной этих сервисов на отечественном рынке и определенным недоверием со стороны заказчиков к размещению своих данных на внешних площадках. Директор по развитию бизнеса SAP компании НОРБИТ Игорь Новиков связывает упомянутую непопулярность облаков тем, что многие клиенты не готовы менять свои процессы под имеющиеся в облачной системе стандарты: «Понятно, что определенный процент кастомизации возможен. Но все же клиенты не готовы менять бизнес-процессы, считая это своим ноу-хау».

Вторым немаловажным фактором является нежелание компаний размещать свои данные на сторонних серверах, считая их в таком случае легкодоступными для конкурентов или представителей органов власти. Очевидно, что для обеспечения роста бизнеса поставщикам придется предоставлять больше технических деталей и информацию о регулирующем законодательстве, чтобы для заказчика все условия использования облачных сервисов были по-настоящему прозрачными и понятными».

И действительно, судя по нашему опросу, полной ясности у заказчиков нет. Так, существенная часть респондентов (47%) ожидает от внедрения

облачных решений сокращения капитальных затрат на ИТ. Однако они не всегда уверены в том, что их бизнес-процессы будут при этом поддерживаться в полной мере. Можно ли использовать облачные среды для тестирования прикладных систем, предшествующего выбору или развертыванию системы? Какие возможности для такого тестирования предлагают сегодня облачные провайдеры?

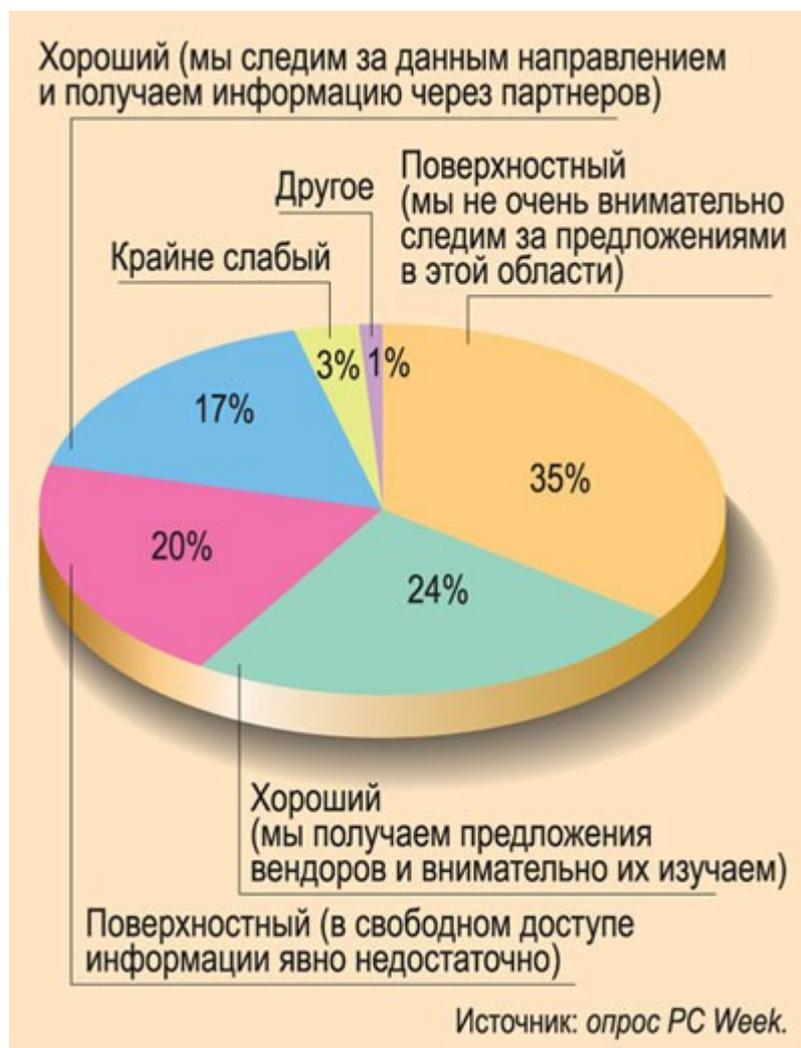


Рис. 3 – Ответы на вопрос: Как вы оцениваете уровень осведомленности вашей компании о предлагаемых в нашей стране альтернативных или дополняющих облачных сервисах для управления бизнесом?

«Важно понимать, что в основе облачных решений лежит концепция упрощения. В стандартном варианте ПО поддерживает базовое количество важнейших настроек, тем самым влияя на снижение ТСО. В облаке можно сделать и разработки, одновременно сохранив преимущества „облачности“. Однако в большинстве случаев это не является стандартным рекомендованным подходом, – предупреждает Павел Растопшин. – В 99% случаев облачное решение дает ожидаемый результат, устраняя проблемы и

принося множество выгод, которые заказчик даже не ожидает получить. Но нередко мы видим, что клиенты опираются на собственные, созданные вручную разработки. Если у них есть сомнения относительно того, сможет ли облачное решение удовлетворить их нужды, SAP предлагает несколько подходов. Для начала проводится демонстрация, основанная непосредственно на бизнес-процессах заказчика, которая, как правило, подтверждает соответствие решения требованиям клиента. Далее клиенты при желании могут тестировать систему еще в течение нескольких дней».

По мнению Артема Третьяка, облачные решения предлагают больше возможностей для предварительного изучения по сравнению с онпремисными. Например, большинство таких решений имеют демо-доступ к полнофункциональной версии, который может быть легко предоставлен по запросу клиента и не требует от него капитальных вложений. Игорь Новиков напоминает, что в России уже есть дата-центры, с помощью которых можно получить доступ к тестовой среде и провести нагрузочные тестирования облачного приложения.

Как считает большинство опрошенных (61%), более широкое использование облачных услуг сдерживается риском прекращения деятельности облачного провайдера. Что можно порекомендовать для уменьшения таких рисков? Михаил Энгельгардт советует детально оценить возможность получения компенсаций в случае одностороннего отказа провайдера в предоставлении услуг по уже заключенному договору и способы/условия выгрузки своих данных. А Артем Третьяк рекомендует выбирать надежную компанию с мировым именем, активно инвестирующую в облачные решения и работающую на российском рынке. «SAP – одна из немногих компаний, которая совместно с „Ростелекомом“ открывает собственный дата-центр и будет предоставлять облачные сервисы из России согласно российским законам», – напоминает Павел Растопшин.

А что будет, если сам заказчик не захочет продлевать контракт? Какие условия предлагаются сегодня компаниям, которые по тем или иным причинам хотели бы отказаться от приобретенных ранее услуг облачного провайдера с наименьшими потерями для себя? Чего в этих условиях недостает, по мнению заказчиков, прежде всего? «Подобный риск не должен стать проблемой для клиента, использующего как онпремисные, так и облачные решения SAP, – убежден Павел Растопшин. – Клиент сам выбирает продолжительность контракта с SAP и партнерами, обычно она составляет 12 мес. Заказчик всегда оставляет за собой право не продлевать контракт. Если клиент принимает такое решение, он не должен платить неустойку и может изъять из системы всю информацию в течение 30 дней после окончания срока договора».

По мнению Михаила Энгельгардта, заказчика в этот момент волнует, что будет с его конфиденциальными данными, и возможно ли промышленными способами их экспортировать в свои системы и/или хранилища данных. Кроме того, услуги по облачным сервисам

предоставляются, как правило, по модели pre-paid, а это автоматически означает что заказчик может гибко планировать срок получения сервиса, но чаще всего не предполагается возврата средств за предоплаченный период. Именно подобного возврата и не хватает многим заказчикам для ощущения финансовой защищенности.

Почти столько же (60%) респондентов смущает перспектива передачи ответственных приложений и данных внешним дата-центрам. Насколько нормативные требования сдерживают широкое применение облачных решений в России? Какие мероприятия наиболее важны для подтверждения легитимности применения облачных сервисов в государственном и коммерческом секторах? «Как правило, отделы безопасности в компаниях разделяют информацию, используемую в различных системах, на классы и уровни доступа в зависимости от потенциальных рисков в случае потери этой информации, — пояснил Михаил Энгельгардт. — Чаще всего по этому же принципу принимают решение и относительно возможности использования на предприятии тех или иных облачных сервисов. Для успеха облачного сервиса в нашей стране ЦОД, обеспечивающий его работу, должен находиться на территории России и быть сертифицирован по международному уровню, не ниже класса TIER3. А сам сервис должен соответствовать нормам 152ФЗ о защите персональных данных и быть сертифицирован по нормам ФСТЭК».

По мнению наших респондентов, есть и другие препятствия на пути более широкого использования облачных услуг. Это отсутствие адекватной финансовой ответственности провайдера за ненадлежащую работу облачного сервиса (49% опрошенных), сложность формулирования SLA-соглашений и подписания соответствующих контрактов (36%), трансграничная передача данных в зарубежные дата-центры (35%), высокая цена сервиса (31%), существенный уровень кастомизации прикладных систем, который сложно поддерживать в облаке (28%), отсутствие прозрачного пути перехода от онпремисных решений к облачным и обратно с сохранением предыдущих лицензионных инвестиций (25%), недостаток примеров успешного использования облачных сервисов в нашей стране (24%) и сложность интеграции облачных и онпремисных решений (20%).

Подобная интеграция многим заказчикам представляется задачей весьма сложной, требующей высокой квалификации и не гарантирующей желаемого результата. Следует иметь в виду, что, согласно нашему опросу, для 39% респондентов побудительным мотивом для развертывания облачных решений является как раз отсутствие в их штате специалистов для развертывания и поддержки технологической платформы на собственной площадке, а следовательно, рассчитывать на собственные силы в деле интеграции им тоже не приходится. Каким условиям должны удовлетворять облачные и унаследованные онпремисные решения в гибридных конфигурациях для того, чтобы их можно было интегрировать в рамках проектов с разумным бюджетом?

«Интеграция облачных и онпремисных решений является одной из сильных сторон облака SAP – это лучшие в своем классе бизнес-решения, которые могут быть интегрированы практически в любую систему, – утверждает Павел Растопшин. – Некоторые облачные решения (SuccessFactors, Ariba) появились в портфеле SAP благодаря приобретениям, и ранее эти приложения интегрировались в любую систему независимо от вендора. Если клиент осуществляет интеграцию облачных и онпремисных решений, мы предлагаем готовую схему, благодаря которой гибридная интеграция проходит всего за несколько дней».

Говоря о технических аспектах, Михаил Энгельгардт напоминает, что в интегрируемых системах в первую очередь должны поддерживаться стандартные форматы обмена данными, такие как плоские файлы, использование API- и Web- сервисов. В идеальной модели решение должно поддерживать и промышленные интеграционные шины, широко используемые в компаниях крупного бизнеса и в госсекторе. «В данном случае вопрос лежит не в плоскости облака/онпремисных решений, а в сложности обмена данными вообще между системами, консистентностью данных, принципами обмена, – соглашается с ним Игорь Новиков. – У ведущих вендоров сейчас имеются инструменты для облегчения интеграции (например, SAP Process Orchestration), которые успешно внедряется в России и позволяют существенно упростить жизнь заказчикам в части обеспечения интеграционных процессов.»



HP HELION CONTINUITY SERVICES: АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ КАК СЕРВИС

Источник: <http://www.pcweek.ru/its/news-company/detail.php?ID=168330>

HP Enterprise Services объявила о выходе улучшений для HP Helion Continuity Services – облачной платформы аварийного восстановления, предлагаемой в виде сервиса (Disaster-Recovery-as-a-Service). Эти улучшения позволят значительно снизить простои, риск потери данных и расходы, связанные с недоступностью системы, а также обеспечат выход платформы на новые рынки.

В связи с ростом востребованности облачных технологий ИТ-специалистам становится все сложнее обеспечивать доступность рабочих нагрузок как в локальной среде, так и в облаке. Восстановление систем должно выполняться за несколько часов, а в критических средах (особенно если речь заходит о возможной потере данных) счет может идти на минуты. Для соответствия таким высоким ожиданиям требуется немалый бюджет,

а также специально обученные специалисты. Хорошо, когда все это есть, но что если организация не может себе этого позволить?

Платформа аварийного восстановления HP, предлагаемая как сервис, позволяет снизить нагрузку на ИТ-отдел. Она обеспечивает следующие преимущества: улучшение показателя времени восстановления до 90%; снижение объема потери данных до 95%; снижение расходов на 15–50% благодаря облачной модели ценообразования.

«Раньше мы сохраняли резервные копии на ленточный носитель. Только так мы могли обеспечить эффективную защиту информации и гарантировать восстановление, – рассказал Барри Алфорд (Barry Alford), руководитель отдела информационных и коммуникационных технологий, Paragon Community Housing Group. – Однако все изменилось, когда мы попробовали новое решение HP. Специалисты компании помогли нам быстро внедрить решение DRaaS. В результате мы усовершенствовали резервное копирование и восстановление, а также повысили производительность».

Улучшенный сервис HP Helion Continuity Service помогает снизить негативное влияние сбоев на бизнес заказчиков. Он защищает рабочие нагрузки, которые запускаются в локальном частном облаке, традиционной среде или в управляемом виртуальном частном облаке HP Helion. В новом выпуске реализована поддержка физических кластеров Linux, включая кластеры Red Hat Enterprise Linux, Oracle Real Application Clusters (RAC) и хранилища данных на базе SAN. Дополнительные улучшения: способность предоставлять дополнительное хранилище во время восстановления в соответствии с меняющимися требованиями рабочих нагрузок; выделенный гипервизор для размещения специализированных приложений, требующих репликации в реальном времени; улучшенная функция создания мгновенных снимков на базе технологии ZPAR обеспечивает гибкость при планировании испытаний; поддержка физических кластеров Linux; поддержка Oracle RAC; хранилища данных на базе SAN; поддержка испытаний для серверов Active Directory.

«Облачные технологии подарили бизнесу фантастические возможности, однако ахиллесовой пятой таких сервисов является отказоустойчивость, – отметил Джим Фанелла (Jim Fanella), вице-президент, Workload and Cloud, HP Enterprise Services. — Мы считаем, что обеспечение непрерывности бизнеса должно стать основной задачей организаций, которые используют облачные технологии. Поставщики облачных сервисов должны гарантировать работоспособность технологий даже при худшем сценарии. Наш портфель сервисов HP Helion в полной мере соответствует требованиям в отношении отказоустойчивости».

Для обеспечения максимальной доступности сервисов и соответствия региональным требованиям HP предоставляет данный сервис в семи центрах восстановления в Северной Америке, Европе и Азиатско-Тихоокеанском регионе.



УПРАВЛЕНИЕ ЭЛЕКТРОННОЙ ПОЧТОЙ В ГОСУДАРСТВЕННЫХ ОРГАНАХ ВЕЛИКОБРИТАНИИ – КОММЕНТАРИИ ГОСУДАРСТВЕННОГО СЛУЖАЩЕГО

Источник: блог «Thinking Records» <http://thinkingrecords.co.uk/2015/03/13/the-management-of-e-mail-in-uk-government-the-comments-of-a-civil-servant/>

Сойдя сегодня с поезда, я наткнулся на своего знакомого – государственного служащего. Уже лет двадцать он работает на достаточно высоком посту, а в последние три года принимал участие в довольно важной инициативе по разработке политики.

Он спросил меня, чем я сейчас занимаюсь. Я ответил, что по-прежнему консультирую по вопросам управления документами, но параллельно начал учиться в аспирантуре и готовить диссертацию. На его вопрос, какую именно тему я выбрал, я рассказал, что изучаю, как государственные органы Великобритании управляют электронной почтой. Он начал смеяться. Не хихикать, заметьте, а именно смеяться, что называется, «от живота».

Я поинтересовался, что тут такого смешного. На это он мне сказал, что, по его мнению, надлежащее управление государственными документами закончилось с ликвидацией бумажных документных систем в конце 1990-х годов. В течение какого-то времени его министерство использовало мощную систему управления электронными документами, но «никто в ней не мог ничего отыскать, и вряд ли кто-либо всерьёз ей пользовался».

Год назад министерство от использования этой электронной системы управления документами отказалось. Были планы внедрить новую систему на основе SharePoint, но они были отложены, так что министерству пришлось обходиться учетными записями электронной почты и общими дисками.

По его словам, в последний раз он что-либо сохранял в какой-либо централизованной документной системе лет пять тому назад.

Вся его переписка идёт по электронной почте. В его учётной записи хранится 11 тысяч сообщений электронной почты. Раньше министерство регулярно проводило уничтожение сообщений электронной почты давностью более 2,5 лет, но эта практика сейчас приостановлена ввиду отказа от использования электронной документной системы.

Я поинтересовался, что он сможет, в случае ухода из министерства или перехода на другую должность, передать своему преемнику. Его ответ был: «почти ничего». По его словам, законченные результаты его работы доступны на веб-сайте министерства, но вот материалы, отражающие ход размышлений и показывающие, как именно он пришёл к этим выводам, будут в таком случае потеряны. Затем он поправил себя, отметив: «на самом

деле потеряны они, конечно, не будут. Они будут лежать где-то на сервере, - их лишь будет практически невозможно отыскать».

Большинство британских государственных органов, судя по всему, удаляет содержимое учетных записей электронной почты спустя несколько месяцев или лет после ухода государственного служащего, так что я подозреваю, что переписка моего знакомого не слишком долго пролежит на сервере в случае его ухода с работы.



ПРАКТИКА ХРАНЕНИЯ ДОКУМЕНТОВ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Источник: <http://esm-journal.ru/docs/Praktika-khraneniya-dokumentov-s-ehlektronnoj-podpisju.aspx>

О практике применения электронной подписи при хранении электронных документов корреспонденту Клерк.Ру Льву Мишкину рассказал Иван Агапов, аналитик компании Synerdocs.

Иван, вот уже целый год мы по закону можем обмениваться электронными документами. Но кроме передачи документов, нам необходимо их хранить и обеспечивать юридическую силу. Закон дает нам электронную подпись, как она помогает обеспечить юридическую значимость хранимых электронных документов?

Начнем с того, что документы имеют свой срок хранения – от пяти лет до нескольких десятилетий. И сам сертификат электронной подписи, который дается сотруднику компании, тоже имеет свой срок действия – как правило, один год. Закон требует, чтобы на момент проверки подписи сертификат либо был действующим, либо должно быть подтверждение, что в момент подписания он был таковым. Если делать проверку подписи спустя год, прямая проверка «в лоб» скажет, что подпись не действительна, поскольку срок сертификата истек.

Как раз этот вопрос и закрывает усовершенствованная электронная подпись. Во-первых, она позволяет доказать время подписания (штамп времени, в котором закреплен момент постановки подписи). Во-вторых, обеспечивает доказательство того, что в конкретное время сертификат действовал и ему можно доверять (списки отзывов, сертификаты из пути доверия).

Так решается принципиальная задача архивного хранения электронного документа – обеспечение юридической значимости документа, чей срок хранения превышает срок действия сертификата электронной подписи.

Сейчас при работе с электронными документами усовершенствованная электронная подпись – единственный гарант юридической силы? Как это отражается в сегодняшней практике, например, в суде?

Конечно, такая подпись – не единственный юридический фактор. Тут стоит вернуться к общей теории признания электронных документов юридически значимыми. Есть много мнений, но мы используем, так сказать, классическую цепочку приоритетов.

Например, у нас есть электронный документ, который мы собираемся использовать в суде, потому следует определить, имеет ли он юридическую значимость. Первое, что суд должен выяснить – может ли он вообще по закону создаваться и существовать в электронном виде. Второе, документ должен содержать все требуемые реквизиты. Третье, суд должен быть уверен, что лицо, которое его подписало, имело право документ подписывать, согласно Уставу, доверенности т.п. Все это фактически является правовым полем документа. И только потом выясняется, действительна ли электронная подпись.

На практике спорный вопрос действительности электронной подписи возникает не часто. Например, суд легко решает проблему с юридической значимостью документа в электронном виде, если стороны ранее заключили соглашение об обмене подписанными электронными документами и даже обменивались ими до возникновения спора. Суд проверяет, прежде всего, наличие факта соглашения об обмене электронными документами, которое фактически закрепляет юридическую силу документа. И только в исключительных случаях суд проверяет действительность самой электронной подписи.

Вернемся к вопросу о хранении электронных документов. Полностью ли электронная подпись решает проблемы обеспечения юридической значимости хранимых данных или какие-то риски сохраняются?

Решает, но не полностью. Закон обязывает нас иметь доказательства, но какие они могут быть – не определено. В нашей практике есть международные стандарты, но это все до сих пор не закреплено законом, потому присутствует потенциальный риск, что в определенный момент государство примет новый стандарт, и текущие технологии придется в корне менять.

Хотя мы склонны считать, что такой риск маловероятен, потому что есть международный опыт и стандарты, которые переделывать не целесообразно. Подтверждением служит и то, что последние предлагаемые поправки в ФЗ-63 «Об электронной подписи» говорят, что законодатели не идут вразрез с практикой.

Плюс к этому у нас сохраняются риски, связанные с самим электронным документом, как таковым. Его тоже нужно как-то хранить, а здесь уже всплывают классические проблемы электронного документа – это носители, это средства хранения и воспроизведения, это форматы и их поддержка. Естественно, что для документов со сроком хранения 5 или 10

лет это не особо актуально, но если мы говорим про документы со сроком хранения в несколько десятков лет, то очень сложно предугадать, что мы будем иметь спустя это время.

В России очень незначительная практика хранения электронных документов. Это не смотря на то, что с 2002 года действует ФЗ-1 «Об ЭЦП» и можно сдавать отчетность в электронном виде, то есть, получается, с электронными архивами мы имеем дело уже больше 10 лет. Правда, отчетность – это специфическая задача, в рамках которой сроки хранения незначительны.

Мы видим, что в практике сохраняется множество противоречий. Что с этим делать операторам электронного документооборота? Возможно, они имеют какое-то решение?

Могу отвечать только за нашу практику. У нас при передаче через сервис документа с электронной подписью, подпись проверяется и доводится до усовершенствованного формата – то есть, мы добавляем штамп времени и другие необходимые параметры. Таким образом, мы обеспечиваем решение задачи обеспечения юридической силой документов с длительным сроком хранения. И в данный момент это единственное подходящее решение.

Даже в этом случае вопрос не решается полностью. Технология электронной подписи тоже имеет свои ограничения, у сертификатов есть сроки действия. Поэтому придется регулярно повторять процедуру подтверждения сертификатов.

А по поводу документов с длительными (например, 50 лет) или постоянными сроками хранения можно вновь сослаться на Европу. Зарубежная практика идет по пути изменения подхода к сохранению в них юридической значимости. Например, упрощаются механизмы обеспечения целостности массива документов. Либо может даже идти речь о переводе в бумажный вид для хранения.

Получается, что по-прежнему главным сдерживающим фактором развития практики хранения электронных документов является законодательство. Помимо обозначенных проблем, каких еще решений вы ждете?

На самом деле все довольно оптимистично. Сегодня у нас уже есть предлагаемые поправки к ФЗ-63, которые несут полезный и позитивный характер, в частности, требования по использованию штампа времени в электронной подписи, вводится понятие о едином пространстве доверия. Это уже хорошо, это уже конкретика. Это влияет на развитие инфраструктуры использования электронной подписи, чтобы пользователь не ломал голову, какой сертификат лучше применять, а приступил к решению своих конкретных задач.

Сейчас сложилась такая ситуация, что зачастую электронная подпись привязана к определенной услуге. С учетом роста разнообразия сервисов, это становится неудобно пользователям. Им нужен один сертификат с максимально широким полем использования. При том, что мы ожидаем

взрывной рост сервисов и областей применения электронной подписи, и если у нас не будет единого пространства доверия, то мы рискуем столкнуться с мощным системным кризисом.

Ну и, самое главное, не решен вопрос с регулированием архивов электронных документов. ФЗ-125 «Об архивном деле» уже устарел, в нем нет практически ничего про электронный документ. Там есть сроки хранения, но ни технологий, ни рекомендаций по электронным документам нет. При том, рынку будет достаточно хотя бы общих принципов и рекомендуемых стандартов, а уже над реализацией он подумает сам. В общем, мы ждем новостей по новому закону, который давно уже всем очень нужен.



**НА САЙТЕ БРИТАНСКОГО ИНСТИТУТА
СТАНДАРТОВ НАЧАТО ПУБЛИЧНОЕ
ОБСУЖДЕНИЕ ПРОЕКТА НОВОЙ РЕДАКЦИИ
СТАНДАРТА ISO/IEC 27000 «СИСТЕМЫ
МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ. ОБЩИЙ ОБЗОР И
ТЕРМИНОЛОГИЯ»**

Источник: сайт Британского института стандартов / сайт ИСО
<http://drafts.bsigroup.com/Home/Details/54287>
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435

С 23 марта 2015 года на сайте Британского института стандартов (BSI) выложен для публичного обсуждения проект очередной редакции ключевого международного стандарта системы менеджмента информационной безопасности ISO/IEC 27000 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (Information technology - Security techniques - Information security management systems - Overview and vocabulary), см. <http://drafts.bsigroup.com/Home/Details/54287> (см. также http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435).

Draft Details**Table of Contents**

- Information technology - Security techniques - ...
- Foreword
- + 0 Introduction
- 1 Scope
- + 2 Terms and definitions
- + 3 Information security management systems
- + 4 ISMS family of standards
- Annex A
- + Annex B
 - B.1 Term ownership
- + B.2 Terms ordered by Standards
- Bibliography

Information technology - Security techniques - Information security management systems - Overview and vocabulary

Number:	ISO/IEC 27000
Type:	DPC
Source:	ISO
Committee:	IST/33/-1
Committee name:	Requirements, security services and guidelines
Review published:	23 Mar 2015
Review end date:	19 May 2015
No. of comments:	0
Categories:	Information coding; character sets

Read Draft Alert a colleague **Draft Scope:**

This International Standard provides the overview of information security management systems, and terms and definitions commonly used in the ISMS family of standards. This International Standard is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

Ранее публичное обсуждение «своей» версии этого документа начал французский орган по стандартизации AFNOR, см. <http://rusrim.blogspot.ru/2015/03/iso-27000.html>.

Новая редакция заменит действующий стандарт ISO/IEC 27000:2014 (см. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411 и <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en>).

Обсуждение на сайте продлится до 19 мая 2015 года.



ПИОНЕР ИНТЕРНЕТА ПРЕДУПРЕЖДАЕТ О ТОМ, ЧТО НАША ЭПОХА МОЖЕТ СТАТЬ «ЭЛЕКТРОННЫМИ ТЕМНЫМИ ВЕКАМИ»

Источник: сайт NPR <http://www.npr.org/blogs/thetwo-way/2015/02/13/386000092/internet-pioneer-warns-our-era-could-become-the-digital-dark-ages>

Что произойдёт, когда самые передовые сегодня системы хранения данных завтра станут рассматриваться как нечто вроде флоппи-дисков?

Ответ на этот вопрос и его последствия для сохранения истории беспокоят вице-президента компании Google Винта Серфа (Vint Cerf). Выступая на ежегодной конференции ведущих американских ученых, Серф

описал подобную утрату важной информации как возможность «электронных Темных веков» («темными веками» в англоязычной литературе называется период средневековья, когда были утрачены многие знания, накопленные древними Грецией и Римом).

Как сообщил журнал «Инженерное дело и технологии» (Engineering and Technology Magazine, E&T, см. <http://eandt.theiet.org/news/2015/feb/vint-cerf-digital-data.cfm>), Серф, выступая в городе Сан-Хосе на ежегодной встрече членов Американской ассоциации содействия развитию науки (American Association for the Advancement of Science), отметил, что, сохраняя в электронном виде все наши книги, документы и фотографии, мы, возможно, тем самым создаем большую проблему для будущих историков, которые захотят изучать события 21-го столетия.

«Если думать о том, что произойдет в будущем через 1000 лет или 3000 лет, нам следует задать себе вопрос: как мы обеспечим долговременную сохранность всех тех битов, которые нужны для правильной интерпретации создаваемых нами электронных объектов?», сказал Серф.

«Мы небрежно, сами того не осознавая сбрасываем все наши данные в то, что может оказаться информационной черной дырой», подчеркнул он.

Данная проблема возникла не вчера: ещё в 2006 году Министерство энергетики США отстегнуло 11 миллионов долларов исследователям из трех университетов и пяти национальных лабораторий в надежде найти решение задачи «управления бурным потоком данных, которые будут созданы следующим поколением суперкомпьютеров». Существуют также компании, предлагающие услуги по преобразованию данных из устаревших систем в форматы, которые сегодня по-прежнему можно использовать.

Как пишет журнал «Инженерное дело и технологии»:

«Сравнивая будущие знания о 21-м веке с после-римским периодом в Западной Европе, о котором известно сравнительно мало из-за отсутствия письменных документов, Серф сказал, что будущие поколения, возможно, также «будут гадать о том, кем мы были», сталкиваясь с большими трудностями в понимании этого из-за тех самых интерпретируемых битов информации, которые мы после себя оставили.

«В своём увлечение оцифровкой мы переводим в электронный вид фотографии, считая, что это обеспечит их более длительную сохранность, - и можем оказаться не правы», - отмети Серф. «Я бы сказал, что если есть фотографии, дальнейшая судьба которых Вас действительно беспокоит, то создайте их экземпляры на физических носителях. Распечатайте их».

В качестве примера Серф ссылается на книгу президентского историка Дорис Кернс Гудвин «Команда соперников: Политическая гений Авраама Линкольна» (Team of Rivals: The Political Genius Of Abraham Lincoln). Готовя её, Гудвин очень существенно опиралась на анализ физических писем, которыми обменивались Линкольн и его современники.

Газета «Телеграф» (The Telegraph) цитирует следующие слова Серфа (см. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/digital-dark->

age-could-leave-historians-with-no-records-of-the-21st-century-10043516.html): «Подобную книгу, возможно, не удастся написать о ныне живущих людях... – необходимый для этого автору книги цифровой контент, такой, как сообщения электронной почты, возможно, «испарится», - либо потому что никто его не сохранил, либо (даже когда сам контент сохранился) из-за того, что его невозможно интерпретировать, поскольку он был создан с помощью программного обеспечения, которому исполнилась сотня лет».

Серф говорит о проблеме создания «электронного пергамента» (digital vellum) и о том, что одним из решений могло стать изготовление электронных «снимков» в момент сохранения объекта, документируя при этом все элементы, необходимые для последующего воспроизведения (включая программное обеспечение и операционную систему). Журнал «Инженерное дело и технологии» пишет:

«Снимок можно было бы затем использовать для воспроизведения игры, изображения или электронной таблицы, на «современном» (в будущем) компьютере, - возможно, столетия спустя.

«Кое-кто говорит, что важные материалы будут скопированы и перенесены на новые носители информации, так зачем беспокоиться?» - сказал Серф. «Но ... историки скажут вам, что порой истинная ценность и значение документов, образов и т.д. может не осознаваться столетиями. Поэтому неспособность сохранить может привести к потере возможности правильно оценить прошлое».



БОЛЬШИЕ ДАННЫЕ: ОСТАВЛЯЯ ПОЗАДИ НЕУДАЧНЫЙ ОПЫТ ПЕРВЫХ ВНЕДРЕНИЙ

Источник: блог Formtek <http://formtek.com/blog/big-data-moving-beyond-the-setbacks-of-early-implementation-failures>

Количество проектов в области «больших данных» растёт, но, к сожалению, многие из подобных проектов до настоящего времени не увенчались успехом. Результаты исследования, проведенного консультационной компанией Cap Gemini (Cracking the Data Conundrum: How Successful Companies Make Big Data Operational – «Решение проблемы данных: Как успешные компании используют большие данные в своей оперативной деятельности», см. http://www.capgemini-consulting.com/resource-file-access/resource/pdf/cracking_the_data_conundrum-big_data_pov_13-1-15_v2.pdf) показали, что только 13% организаций смогли включить «большие данные» в проект, принятый в промышленную эксплуатацию; и лишь 27%

использующих «большие данные» коммерческих организаций сообщили об успешности таких проектов.

Согласно отчету Cargemini, отчасти неудачи проектов использования «больших данных» были связаны с плохо поставленными целями и задачами, и с отсутствием предварительного планирования хода реализации проектов. Вице-президент североамериканского отделения CarGemini Джефф Хантер (Jeff Hunter) отметил, что «в целом, это несоответствие между тем, что получается на выходе, и четко определенными деловыми движущими силами и целями. И на этом пути люди «окунаются» в технологии. Мы видим, что успешные компании централизовали концепцию применения технологий «больших данных», достижений науки о данных и аналитики. Именно они продвигаются быстрее».

Тем не менее, несмотря на все проблемы с ранними попытками внедрения относительно новой технологии, есть место для оптимизма. Хантер сказал, что «Я вижу начало того же цикла, что и с Интернетом и электронной коммерцией. В рамках всего сообщества лишь несколько компаний добиваются успеха. Те, кто осваивает «большие данные» - даже те, кто проходит через неудачи и провалы, - [накапливают опыт]. Они видят, что движимый данными процесс принятия решений имеет свою нишу в деловой деятельности. Успешные проекты станут катализатором, ускоряющим появление других проектов».



ТРЕБОВАНИЯ К ПОРЯДКУ МЕЖВЕДОМСТВЕННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ПРИ ПРЕДОСТАВЛЕНИИ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ И ИСПОЛНЕНИИ ФУНКЦИЙ В ЭЛЕКТРОННОЙ ФОРМЕ

Источник: Консультант Плюс <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=137721>

Приказом Министерства связи и массовых коммуникаций РФ от 20 января 2015 года № 9 утверждены «Требования к порядку межведомственного информационного взаимодействия при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме».

Согласно приказу, **требования являются обязательными для исполнения** при разработке порядка межведомственного информационного взаимодействия при предоставлении государственных и муниципальных

услуг и исполнении государственных и муниципальных функций в электронной форме (п.2 Приказа). До 1 декабря 2015 года министерством должен быть подготовлен проект такого порядка.

Требования устанавливают содержание нормативно-правового акта - «Порядок межведомственного информационного взаимодействия при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме, осуществляемого с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме».

Порядок должен включать следующие основные положения (п.3):

- Перечень участников межведомственного информационного взаимодействия;
- Условия межведомственного информационного взаимодействия;
- Порядок доступа к информации, размещаемой в инфраструктуре взаимодействия;
- Порядок приема в электронной форме запросов, обращений, заявлений и иных документов, поступающих с использованием инфраструктуры взаимодействия, а также порядок и сроки их обработки и подготовки ответов в электронной форме;
- Требования к техническим средствам, обеспечивающим фиксацию даты, времени и участников каждого случая взаимодействия, а также возможность предоставления сведений, позволяющих восстановить историю взаимодействия;
- Срок рассмотрения обращений о сбоях и нарушениях функционирования инфраструктуры взаимодействия и ее элементов, а также случаев нарушения требований об обеспечении информационной безопасности;
- Требования к совместимости технологий, используемых в информационных системах органов и организаций при таком взаимодействии;
- Обеспечение защиты передаваемых сведений от неправомерного доступа, уничтожения, модификации, блокирования, копирования, распространения, иных неправомерных действий;
- Обеспечение соблюдения конфиденциальности информации ограниченного доступа в соответствии с требованиями законодательства РФ;
- Иные требования, определяемые федеральными законами, правовыми актами Президента РФ и нормативными правовыми актами Правительства РФ.

Установление таких требований можно расценивать как шаг в правильном направлении, поскольку требования позволяют

стандартизировать массово разрабатываемые и утверждаемые ведомственные нормативно-правовые акты (НПА).

Согласно приказу, требования являются обязательными. Интересно будет посмотреть, кто будет проверять ведомственные НПА на соответствие им, и что будет тем ведомствам, которые эти требования частично проигнорируют.



АВСТРАЛИЙСКИЙ ОПЫТ ПРОВЕДЕНИЯ САМООЦЕНКИ ЭЛЕКТРОННОГО ХРАНИЛИЩА УЧРЕЖДЕНИЯ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ К ДОВЕРЕННЫМ ХРАНИЛИЩАМ СТАНДАРТА ISO 16363-2012

Источник: сайт журнала D-Lib Magazine <http://www.dlib.org/dlib/march15/houghton/03houghton.html>

Автор: Наташа Храмцовская

Статья Бернадетт Хоутон из австралийского университета Дикин (Deakin University) под названием "Trustworthiness: Self-assessment of an Institutional Repository against ISO 16363-2012" была опубликована в электронном журнале D-Lib Magazine (том 21, номер 3-4 за март-апрель 2015 года, <http://www.dlib.org/dlib/march15/houghton/03houghton.html>). Вниманию читателей предлагается краткая «выжимка» из неё, отражающая основные результаты.

О международном стандарте ISO 16363:2012 «Системы передачи данных и информации о космическом пространстве – Аудит и сертификация доверенных электронных хранилищ» (Space data and information transfer systems - Audit and certification of trustworthy digital repositories) см. также <http://rusrim.blogspot.ru/2012/02/iso-163632012.html>.

Сегодня почти все создаваемые нами документы и результаты практически всех научно-исследовательских проектов являются электронными объектами. Не все их нужно хранить постоянно, однако представляющие научную или историческую ценность материалы должны быть сохранены для будущих поколений. Обеспечение долговременной сохранности электронных объектов является более сложным делом, чем сохранение материалов на бумаге: оборудование устаревает, новое программное обеспечение заменяет старое, носители информации деградируют.

В последние годы был достигнут значительный прогресс в разработке инструментов и стандартов по обеспечению долговременной сохранности электронных носителей информации, в частности, в контексте электронных хранилищ учреждений. Пока что наиболее широко распространенным стандартом является документ под названием «Аудит и сертификация доверенных хранилищ: Критерии и контрольный список» (Trustworthy Repositories Audit and Certification: Criteria and Checklist), сокращенно TRAC, на основе которого был разработан международный стандарт ISO 16363-2012.

Библиотека университета Дикин (Deakin University Library) провела самооценку на соответствие критериям стандарта ISO 16363. Квинтэссцией этого опыта стала настоящая статья, в которой дана оценка стандарту ISO 16363, описан процесс самооценки и приведены рекомендации для всех тех, кто хотел бы осуществить аналогичные проекты.

В целом, самооценка оказалась трудоемким и ресурсоемким, но полезным мероприятием, в ходе которого был выявлен ряд слабых мест в настройках и рабочих процессах электронного хранилища библиотеки «Система онлайн-доступа к научно-исследовательским данным университета Дикин» (Deakin Research Online, DRO, <http://dro.deakin.edu.au/>). Впоследствии был разработан стратегический план по устранению этих недостатков, и, как следствие, повышение степени доверия к хранилищу DRO. Предполагается, что регулярные повторные самооценки будут проводиться раз в три года; при этом ожидается, что они уже не будут столь ресурсоемкими, как первичная самооценка, поскольку соответствующая документация уже была выявлена, и было установлено её местоположение.

Мы настоятельно рекомендуем другим библиотекам в какой-то момент провести аналогичную самооценку их хранилищ, выбирая инструменты для этого и глубину самооценки в зависимости от размера библиотеки и от имеющихся ресурсов. Исследователи рассчитывают на то, что их публикации будут в безопасности в хранилищах учреждений, и руководству хранилищ необходимо обеспечить, чтобы хранилища соответствовали этим ожиданиям. Самооценка является одним из механизмов, позволяющих убедиться в том, что их хранилище действительно может считаться доверенным.

Основываясь на опыте университета Дикин, мы рекомендуем руководителям хранилищ, которые планируют провести самооценку на соответствие ISO 16363, следующее:

- Проводить самооценку прежде, чем решать вопрос об оплате внешней сертификации. Сертификация - и переаттестация – дорогие удовольствия;
- Заручиться поддержкой высшего руководства. Такая поддержка имеет решающее значение. Обеспечение долговременной сохранности требует длительных усилий;
- Лицо, проводящее самооценку, должно быть достаточно хорошо знакомо с политиками и процедурами организации и хранилища;

- Если у Вас нет времени или ресурсов для проведения оценки на соответствие ISO 16363, подумайте о проведении оценки на соответствие «Уровням обеспечения электронной сохранности» Национального альянса попечения об электронных материалах (NDSA Levels of Preservation, 2012), <http://www.digitalpreservation.gov/ndsa/activities/levels.html> (см. также мой пост http://rusrim.blogspot.ru/2012/11/blog-post_9881.html - Н.Х.).
- Настроить вики-ресурс для документирования результатов самооценки. Сделайте это следует в начале проекта, и затем документировать результаты по мере продвижения;
- Спланировать проект самооценки с учетом рисков и доступного времени и ресурсов;
- Заранее определить глубину самооценки. Будет ли, например, проводящий оценку специалист просто собирать и анализировать документацию, или же он будет также проводить проверки с тем, чтобы убедиться, что документированные процедуры реально исполняются и что все «спрятанные под капотом» механизмы работают должным образом?
- Использовать при сборе документации знания, имеющиеся у специалистов на местах. Содержащийся в стандарте ISO 16363 список «рекомендуемых доказательств» - это всего лишь рекомендации;
- Лучше познакомиться с критериями, прежде чем начинать самооценку. Определенную документацию можно использовать для того, чтобы удовлетворить нескольким критериям, и если такие критерии выявить на ранних стадиях проекта, то можно будет сэкономить время;
- Помните, что не все критерии ISO 16363 будут применимы в Ваших конкретных условиях;
- Не останавливайтесь. Завершение самооценки не означает, что тяжелая работа уже позади. Потребуется осуществить ряд улучшений. Поставьте перед собой задачу с течением времени повысить жизнеспособность Вашего хранилища;
- Запланируйте регулярное проведение повторных самооценок;
- Если Вы планируете в будущем провести самооценку на соответствие требованиям ISO 16363, начните этот процесс прямо сейчас. Создайте вики-страницу, где Вы сможете фиксировать сведения о соответствующей документации, которая Вам будет попадаться. Ведите список проблем, связанных с обеспечением долговременной сохранности, и обновляйте вики-страницу по мере необходимости, чтобы сэкономить время в дальнейшем;
- Не считайте, что если программное обеспечение Вашего хранилища соответствует стандарту OAIS, то и само Ваше хранилище также будет ему соответствовать. Рабочие процессы и настройки хранилища способны как обеспечить соответствие стандарту OAIS, так и нарушить его;
- Не все перечисленные в ISO 16363 критерии в равной степени важны или связаны с одинаковыми уровнями риска. Оцените должным образом важность каждого критерия;

- Стандарт ISO 16363 основан на концептуальной модели (модели OAIS). Не ждите, что его критерии обязательно будут согласовываться с индивидуальными настройками и рабочими процессами Вашего хранилища.



США: ШУМ ПО ПОВОДУ ЭЛЕКТРОННОЙ ПЕРЕПИСКИ ХИЛЛАРИ КЛИНТОН И СКРЫТАЯ ЗА НИМ СКАНДАЛЬНАЯ ПРОБЛЕМА

Источник: сайт веб-журнала Slate http://www.slate.com/articles/news_and_politics/war_stories/2015/03/the_national_archives_has_failed_to_keep_up_with_digital_records_its_incompetence.html

Данная статья Фреда Каплана была опубликована в веб-журнале Slate 16 марта 2015 года под названием «The Real Scandal Behind Hillary Clinton's Email». Поводом для неё послужил разгорающийся в США скандал, связанный с тем, что Хиллари Клинтон (Hillary Clinton), во время пребывания на посту государственного секретаря, в нарушение законодательства вела свою электронную переписку не через подконтрольный государству почтовый сервер, а через собственный, в результате чего потенциально могли быть уничтожены подлежащие постоянному хранению государственные документы и допущена утечка секретной информации. Само собой, что масло в огонь активно подливают политические оппоненты Клинтон от демократической партии.

Мы теряем целый пласт исторических документов из-за того, что Национальные Архивы провалили свою работу.

Уже стало ясно, что скандальная ситуация, связанная с уклонением Хиллари Клинтон от соблюдения правил работы с электронной почтой, не является изолированным случаем. Прочтите второй абзац статьи, опубликованной на первой полосе газеты Нью-Йорк Таймс за 14 марта 2015 года, озаглавленной «Электронные письма Клинтон, которые, как она уверяет, были сохранены, на деле могли быть утрачены» (Emails Clinton Said Were Kept Could Be Lost):

Хиллари Клинтон не единственная, кто небрежно относится к сохранению исторического наследия. Фото Lucas Jackson / Reuters.

"Но в эту пятницу Государственный департамент признал, что вплоть до начала последнего месяца у него не было никакой возможности обеспечить регулярное сохранение электронной почты представителей высшего руководства. Вместо этого ведомство полагалось на отдельных работников, которые должны были принимать решения о том, следует ли

считать конкретные электронные письма государственными документами, и если да, то перемещать их на специальный сервер для хранения документации, либо распечатывать их и вручную подшивать в дела для обеспечения их долговременной сохранности".

После этого статья в «Таймс» возвращается к саге о частной учетной записи электронной почты Клинтон, но по-настоящему захватывающая дух история, имеющая длительные последствия, сконцентрирована именно в этих двух предложениях. Государственный департамент ничего не делает для того, чтобы сохранить государственные документы. Как рассказывают мне люди, ничего не предпринимают и другие федеральные бюрократические учреждения. В результате наша история улетучивается в пустоту. Здесь и сейчас принимаются важнейшие решения - вершатся события, преобразующие мир - но их причины, возможно, никогда не станут известными.

В старые времена чиновники писали или надиктовывали друг другу меморандумы. Секретари печатали меморандумы под копирку в 3-4 экземплярах, и копии помещали в дела. Периодически кто-нибудь из сотрудников Национальных Архивов приходил с тележкой и вывозил копии для передачи на архивное хранение.

В результате сегодня можно писать книги о войне во Вьетнаме, о Второй мировой войне и о многих других событиях, больших и малых. Историки могут пойти в архивы и прочитать меморандумы, которыми обменивались министр обороны Роберт Макнамара и советник Президента по национальной безопасности Макджордж Банди – значительная часть «бумаг Пентагона» состоит из некогда секретных меморандумов такого рода. Они могут прочесть переписку между Франклином Д. Рузвельтом и Уинстоном Черчиллем и военные планы генералов союзных сил.

В течение последних двух десятилетий подобные документы если и сохранялись вообще, то нерегулярно и не в полном объёме. Проблема заключалась в том, что Национальные Архивы США медлили с установлением норм и правил хранения и формирования в дела электронных документов – и ещё больше медлили с мерами, обеспечивающими исполнение этих правил.

В 2000-м году Национальные Архивы приступили к разработке системы «Архив электронных документов» (Electronic Records Archives, проект ERA), и в 2008 году началось финансирование пилотных программ, но в эксплуатацию система была введена лишь в 2012 году. До этого момента, у Национальных Архивов не было никаких возможностей для работы с документами в формате Microsoft Word, с PowerPoint-презентациями и с сообщениями электронной почты с присоединенными файлами. *(Национальные Архивы уже много лет собирают и хранят огромное количество электронных объектов, но, конечно же, система ERA намного расширила их возможности в этом отношении).* Даже сейчас, как показывает публикация в «Таймс», соответствующие протоколы и

процедуры не внедрены в полной мере в практику работы. В значительной степени это всё ещё незаконченная работа; некоторые элементы новой программы планируются ввести лишь в конце следующего года.

Наша история улетучивается в пустоту

В отчете о результатах внутреннего аудита, написанном официальными лицами Национальных Архивов в 2005 году (рассекречен в 2009 году, о нем см. http://www.slate.com/articles/news_and_politics/war_stories/2009/01/powerpoint_to_the_people.html) сделан вывод о том, что уничтожение и передача на архивное хранение электронных документов «как правило, проводились не в соответствии» с требованиями федеральных нормативных актов и, в частности, многие электронные письма были «уничтожены преждевременно».

Авторы отчета указали несколько причин такого положения дел. Во-первых, ряд чиновников готовил электронные письма на личных компьютерах (Клинтон была не первой, кто так делал, но она, возможно, стала первой, кто поступал только так). Во-вторых, «из-за того, что электронные документы менее «материальны», чем документы на бумажных носителях», государственные служащие, как правило, не склонны были рассматривать их как «документы, требующими надлежащего размещения в дела и решения их дальнейшей судьбы». В-третьих, во многих органах и подразделениях обязанности «хранителя документов» (*ответственного за делопроизводство или архивиста*) часто передавались от одного сотрудника другому, и нередко их в течение длительного времени вообще никто не исполнял. Когда, наконец, подбирали такого человека, никто не уведомлял об этом Национальные Архивы, и у тех не было возможности организовать обучение хранителей. Наконец, несмотря на экспоненциальный рост объёмов электронных документов в последние годы, количество хранителей документов «существенно» уменьшилось.

Судя по всему, с тех пор мало что изменилось. Один архивист рассказал мне, что никто так и не решил вопрос о том, как сохранять файлы, присоединенные к сообщениям электронной почты. Национальные Архивы также не требуют от ведомств готовить пояснительные тексты к PowerPoint-презентациям – что является серьёзной ошибкой, учитывая то, что PowerPoint-презентации давно уже очень широко используются силовыми структурами и разведывательным сообществом.

Короче говоря, наша история по-прежнему утекает сквозь пальцы. Многие из делающих историю лиц (а не только Клинтон) игнорируют свои обязанности по сохранению исторического наследия, в то время как архивисты, которым поручено обеспечить сохранность истории, лишь пожимают плечами и позволяют этим материалам исчезать.

Это трудная задача: сообщения электронной почты мимолетны; жесткие диски отказывают; и нет электронного эквивалента сделанных под копирку экземпляров. И если не заметно, чтобы Национальные Архивы

предпринимали серьёзные усилия по сохранению всех этих сокровищ, то почему кто-то ещё должен беспокоиться по этому поводу?

Старый профессор истории, у которого я учился в колледже, когда его спросили о том, разумно ли пытаться сделать профессиональную карьеру в этой области, покачал головой и сказал, «Заниматься историей бесперспективно». Сегодня он мог бы добавить: «В будущем вообще не будет никакой истории».



НАЦИОНАЛЬНЫЕ АРХИВЫ США ИСПОЛЬЗУЮТ РЕШЕНИЕ «ЕДИНЫЙ АРХИВ» КОМПАНИИ ZL TECHNOLOGIES ДЛЯ УПРАВЛЕНИЯ НЕСТРУКТУРИРОВАННЫМИ ДАННЫМИ

Источник: сайт Digital Journal, <http://www.digitaljournal.com/pr/2505657>

Компания ZL Technologies, Inc. (<http://www.zlti.com>) 26 марта 2015 года объявила о том, что её продукт «Единый архив» (ZL Unified Archive®, ZL UA, <http://www.zlti.com/unified-archive>) в настоящее время применяется Национальными Архивами США (National Archives and Records Administration, NARA) для решения задач управления документами и информацией в отношении государственных неструктурированных данных. Данный продукт является частью разработанного системным интегратором - фирмой Unisys Corp. решения, обеспечивающего переход Национальных Архивов на использование облачной электронной почты и системы коллективной работы.

Для справки: На своём сайте компания ZL Technologies пишет; «Решение ZL UA не имеет себе равных в плане масштабируемости и поддержки детального управления и контроля над неструктурированным контентом. Подход, при котором существует единственный экземпляр данных, один централизованный механизм отслеживания сроков хранения и единое хранилище для всех типов данных, обеспечивает всеохватывающее управление.

Как лидер в области архивации и управления неструктурированными «большими данными» для крупных предприятий, компания ZL, как никто, способна обеспечить выполнение требований по безопасности и масштабируемости ведомства, которому необходим потенциал для архивирования больших объёмов исторически значимых документов, дел, официальных электронных писем и других соответствующих материалов.

В ноябре 2011 года президент Обама подписал президентский Меморандум по управлению государственными документами, тем самым

официально обозначив начало работы над директивой для исполнительной ветви власти, содержащей концепцию перевода в электронный вид государственных документов постоянного срока хранения.

Чтобы соблюсти требования Меморандума при переходе на использование облачной электронной почты, Национальным Архивам потребовались как масштабируемость (для того, чтобы удовлетворить потребности в хранении больших объемов данных), так и возможность продемонстрировать исполнение ими в полном объеме федеральных законодательно-нормативных требований к управлению документами.

Обслуживающий Национальные Архивы системный интегратор – фирма Unisys, рассмотрела возможность использования решения ZL UA в качестве всеохватывающей платформы для неструктурированных данных, обеспечивающей выполнение требований по безопасности стандарта DoD 5015.2 для всех основных почтовых клиентов (включая Google Mail (Gmail) в облаке); и пришла к выводу, что это отличный вариант для выполнения строгих требований Национальных Архивов.

«То, что Национальные Архивы придают такой приоритет единому подходу, посылает недвусмысленный сигнал государственному и частному секторам о том, что изолированные решения более не являются жизнеспособными в условиях, когда в геометрической прогрессии растут как объемы, так и значимость неструктурированных данных», - говорит генеральный директор компании ZL Technologies Кон Леон (Kon Leong). «Единая платформа, единственный экземпляр данных и единая точка контроля позволяют организациям получить всеобъемлющее представление о своей неструктурированной информации, одновременно обеспечивая полномасштабное управление данными с целью удовлетворения потребностей в областях управления документами и информацией, э-раскрытия, исполнения законодательно-нормативных требований и предоставления доступа для общественности».



КОГДА (НЕ) НУЖНО МИГРИРОВАТЬ С ФОРМАТА PDF НА PDF/A

Автор: Наташа Храмцовская

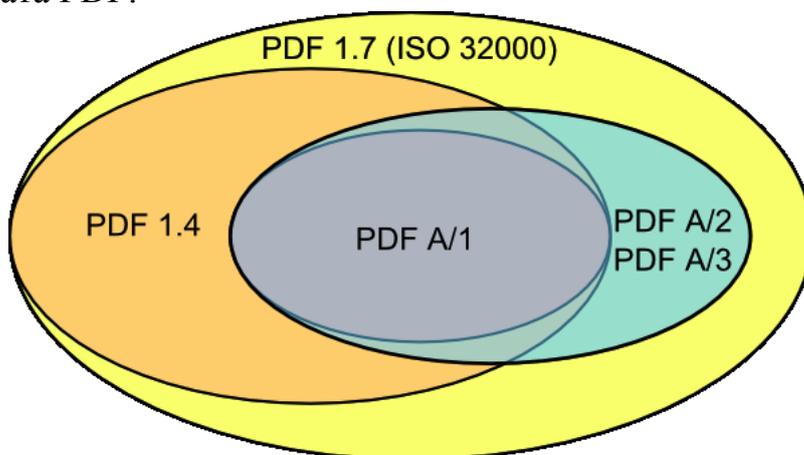
Хорошо известно, что PDF-документы могут содержать элементы и механизмы, чреватые рисками при обеспечении долговременной сохранности (на эту тему см., например:

<https://web.archive.org/web/20130515073645/http://libraries.stackexchange.com/questions/964/what-preservation-risks-are-associated-with-the-pdf-file-format> и <http://wiki.opf-labs.org/display/TR/Portable+Document+Format>).

Миграцию существующих PDF-файлов в формат PDF/A иногда продвигают в качестве стратегии смягчения этих рисков. Преимущества такого подхода, однако, часто весьма сомнительны, и процесс миграции сам по себе может быть довольно рискованной операцией. Поскольку мне часто задают вопросы по этой теме, я подумал, что имеет смысл коротко изложить свою позицию.

PDF/A – это профиль

Во-первых, важно подчеркнуть, что каждый из стандартов формата PDF/A (A-1, A-2 и A-3) на самом деле всего лишь профиль (вариант) использования «полного» формата PDF. Если говорить более подробно, то PDF/A-1 представляет собой подмножество формата PDF версии 1.4, в то время, как PDF/A-2 и PDF/A-3 основаны на версии формата PDF 1.7, зафиксированной в стандарте ISO 32000. Общим у этих профилей является то, что они запрещают некоторые функциональные возможности (например, мультимедийные элементы, шифрование, интерактивный контент), допускаемые в «обычном» формате PDF. Кроме того, они сужают выбор способов реализации ряда других функциональных возможностей - например, требуя, чтобы все шрифты были встроенными (embedded). Это иллюстрирует приведенная ниже диаграмма, показывающая соотношение наборов функциональных возможностей упомянутых разновидностей формата PDF.



Видно, что формат PDF/A-1 является подмножеством формата PDF 1.4, который, в свою очередь, является подмножеством PDF 1.7. Форматы PDF A/2 и PDF A/3 (показанные вместе, чтобы не усложнять диаграмму) представляют собой подмножества формата PDF 1.7 и включают все функциональные возможности формата PDF A/1.

Имея это в виду, нетрудно увидеть, что миграция произвольного PDF-файла в формат PDF/A легко может привести к проблемам.

Потери и изменения в процессе миграции

Предположим, что у нас имеется PDF-файл, содержащий видеоклип. Такая возможность запрещена в PDF/A, поэтому миграция в PDF/A просто приведет к потере мультимедийного контента. Ещё одним примером могут служить шрифты: в PDF/A документе все шрифты должен быть

встроенными. Но что произойдёт в случае, если в исходном PDF-файле используются внешние (невстроенные) шрифты, недоступные на том компьютере, на котором выполняется миграция? Прекратит ли инструмент миграции обработку файла с выдачей предупреждения, или же молча будет использовать какой-то альтернативный (возможно, аналогичный по параметрам) шрифт? Как это проверить?

Сложность структуры и последствия имеющихся ошибок

Кроме того, такого рода миграции, как правило, включают полную повторную обработку внутренней структуры PDF-файла. Сложность данного формата означает наличие большого потенциала для того, чтобы в ходе процесса миграции что-то пошло не так – особенно в случае, когда исходный PDF-файл содержит неочевидные ошибки, и в этом случае риск потери информации вполне реален (даже если исходный документ прекрасно отображается программой просмотра). Так как у нас практически нет инструментов для обнаружения подобных ошибок (т.е. нет достаточно надежных программ, проверяющих структуру PDF-файлов), то обработка таких ситуаций может оказаться непростым делом. Некоторые дополнительные соображения можно найти в публикации по адресу <http://web.archive.org/web/20130605142355/http://libraries.stackexchange.com/questions/1117/convert-ing-invalid-pdfs-or-not-for-digital-preservation> (контекст там несколько отличается, но риски похожи).

Оцифрованные и изначально-электронные документы

Ещё одним фактором, который в ряде случаев потребует принять во внимание, является происхождение исходных PDF-файлов. Если PDF-файлы были первоначально созданы в рамках проекта оцифровки (например, отсканированные книги), то такие PDF-файлы, как правило, не более чем оболочка для набора графических образов, возможно, дополненного слоем распознанного текста. Миграция таких PDF-файлов в формат PDF/A довольно проста, так как исходные файлы вряд ли будут содержать какие-либо объекты, использование которых не разрешено в PDF/A. Одновременно это также означает и ограниченность отдачи от миграции таких файлов в формат PDF/A, так как исходные PDF-файлы изначально не были проблемными!

Потенциальные преимущества формата PDF/A может быть более очевидными в отношении многих видов изначально-электронного контента. В то же время, по причинам, перечисленным в предыдущем разделе, миграция в этом случае является более сложным делом, и есть масса всего другого, что может пойти не так (некоторые дополнительные соображения см. также здесь: <http://qanda.digipres.org/19/what-are-the-benefits-and-risks-of-using-the-pdf-a-file-format?show=21#a21>).

Выводы

Хотя идея миграции PDF-документов в формат PDF/A может казаться чрезвычайно привлекательной, делать это на практике на самом деле довольно рискованно, и такая миграция легко может привести к

непреднамеренной потере данных. Более того, риски возрастают с увеличением числа недружественных в плане электронной сохранности особенностей, и это означает, что миграцию, скорее всего, успешно пройдут те исходные PDF-файлы, с которыми с самого начала не было проблем – и это ставит под сомнение саму цель преобразования в формат PDF/A. В конкретных случаях миграция в PDF/A может оказаться разумным подходом, но при этом ожидаемую отдачу следует тщательно сопоставить с рисками. В отсутствие стабильных, общепринятых инструментов для оценки качества PDF-файлов (как исходных, так и полученных в результате миграции), также представляется разумным всегда сохранять исходные PDF-файлы.

Йохан ван дер Книйф (Johan van der Knijff)

Мой комментарий: С моей точки зрения, голландский специалист несколько сгущает краски. Риск неудачной миграции есть всегда, поэтому в серьёзных проектах обязательно предусматривается тщательный контроль качества и принятие, в случае необходимости, корректирующих мер. Но ван дер Книйф совершенно прав в том, что всегда, начиная проект миграции, полезно оценивать риски (в том числе экспериментально), и сопоставлять ожидаемую на длительном интервале времени отдачу с затратами и рисками.

Как мне кажется, нашим специалистам особенно полезно познакомиться с соображениями голландского коллеги именно сейчас, когда в Минкомсвязи зародилась идея сделать формат PDF/A стандартным для наших органов государственной власти.



ДАНИЯ: ОТКРЫЛСЯ КРУПНЕЙШИЙ ЦИФРОВОЙ АРХИВ СТРАНЫ

Источник: сайт газеты The Copenhagen Post <http://cphpost.dk/news/new-article.12735.html>

Автор: Люси Рюхла

Страна получила бесплатный доступ к миллионам документов, некоторые из которых датируются 1600-ми годами.

20 февраля 2015 года в 4 вечера для широкой публики был открыт крупнейший в Дании цифровой фотоальбом, содержащий почти два миллиона изображений. Датчане могут получить доступ к онлайн-базе данных на сайте Arkiv.dk (<http://arkiv.dk/>), включающей 1841254 документов, таких как фотографии, дневники, письма, звуко- и видеозаписи.

Начиная с конца 1980-х годов, все материалы из более чем 550 архивов страны были переведены в электронный вид, и теперь большая часть из них стала свободно доступной для общественности.



В датских архивах хранится около 50 миллионов изображений и более 100 погонных километров документов, которые будут выложены на электронной платформе (Фото: Wikipedia)

arkivdk

Tilbage

News, find, begrebet, find

Sandvadgård, Vongevej 35

Sandvadgård, Vongevej 35

Nummer	81181
Type	Billeder
Bemærkning	N
Periode	1900 - 1923
Dateringsnote	Før 1923
Materiale	s/h pos. 12x18 cm
Sogn	Hvejsel Sogn
Kommune	Veje Kommune
Arkiv	Lokalhistorisk Arkiv i Jelling

Søg videre i Lokalhistorisk Arkiv i Jelling

om arkiv.dk | om arkiverne | ofte stillede spørgsmål | kontakt

Датское культурное наследие

По оценке Ассоциации местных архивов, датские архивы в общей сложности хранят около 50 миллионов изображений и более 100 погонных километров полок с оригиналами документов.

Каждый месяц в базу будут добавляться 25 тысяч новых фотографий.

«Это величайший день в моей профессиональной жизни, а я работаю архивистом с 1980 года», - говорит Йорген Томсен, архивист из города Оденсе. «Становится общедоступной важная часть культурного наследия Дании».

Благодарность фонду Мёллеров

На все документы электронного архива, самые старые из которых датируются 1600-ми годами, распространяются общие правила защиты авторских прав.

В 2013 году фонд Мёллеров (AP Møller, Chastine Mc-Kinney-Møller) пожертвовал архиву 1,8 миллиона датских крон, что позволило покрыть две трети расходов на создание веб-сайта.

ЗМІСТ

Передмова.....	1
Гибридный подход в обеспечении сохранности и доступности документов.....	3
Как решать проблему длительного хранения документов с учетом устаревания форматов и носителей?.....	8
Проблемы и перспективы облаков: мнение читателей PC Week, комментарии экспертов.....	9
Ир helion continuity services: аварийное восстановление как сервис.....	15
Управление электронной почтой в государственных органах Великобритании – комментарии государственного служащего.....	17
Практика хранения документов с электронной подписью.....	18
На сайте Британского института стандартов начато публичное обсуждение проекта новой редакции стандарта ISO/IEC 27000 «Системы менеджмента информационной безопасности. Общий обзор и терминология».....	21
Пионер Интернета предупреждает о том, что наша эпоха может стать «электронными темными веками».....	22
Большие данные: Оставляя позади неудачный опыт первых внедрений...	24
Требования к порядку межведомственного информационного взаимодействия при предоставлении государственных и муниципальных услуг и исполнении функций в электронной форме.....	25
Австралийский опыт проведения самооценки электронного хранилища учреждения на соответствие требованиям к доверенным хранилищам стандарта ISO 16363-2012.....	27
США: Шум по поводу электронной переписки Хилари Клинтон и скрытая за ним скандальная проблема	30
Национальные Архивы США используют решение «Единый архив» компании ZL Technologies для управления неструктурированными данными.....	33
Когда (не) нужно мигрировать с формата PDF на PDF/A.....	34
Дания: Открылся крупнейший цифровой архив страны.....	37