ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо зберігання і використання електронної інформації в сучасному інформаційному суспільстві.

У публікації «Германия: Электронный промежуточный архив DZAB» наведені результати пошуку керівних документів та інформації щодо створення та організації роботи проміжного електронного архіву Германії DZAB.

У публікації «Вопрос коллеги: С чего начинать создание электронного архива?» наведено заходи які необхідно виконати під час створення електронного архіву установи.

У публікації «Вопрос коллеги: Отказ от документов на бумажных носителях» розповідається про досвід та наведено керівні документи які допоможуть відмовитись від паперового документообігу.

У публікації «Изучение проблемы подтверждения аутентичности электронных документов: Первые результаты проведенного исследования» наведено інформацію про окремі заходи щодо підтвердження аутентичності електронних документів.

У публікації «США: Новые функциональные возможности электронной почты и их последствия для управления документами» розповідається про заходи щодо забезпечення «конфіденційного режиму» електронної пошти Google.

У публікації «Документационный анализ – процесс установления требований к захвату и срокам хранения документов» розповідається що таке документаційний аналіз, наведено критерії експертизи цінності документів.

У публікації «Проблемы хранения электронных научно-технических документов» розповідається що цю роботу проводять фахівці РДАНТД, надано ссилку на доповідь з цього питання.

У публікації «Новый британский стандарт BS 10754-1:2018 обеспечения доверия к системам, программному обеспечению и услугам» розповідається про зміст стандарту.

У публікації «Электронная архивация: «Контекст – это наше всё»» розповідається про особливості каталогізації електронних документів.

У публікації «Документы и данные в облаке: Проблемы этики и доверия» розповідається про інструменти розроблені в ході проекту InterPARES Trust з метою оцінити переваги і ризики хмарних послуг.

У публікації «Перелік міжнародних стандартів, які опрацьовано та проаналізовано НДІ мікрографії за І півріччя 2018 року», наведено перелік міжнародних стандартів, які опрацьовано та проаналізовано співробітниками НДІ мікрографії у І півріччі 2018 року.

ГЕРМАНИЯ: ЭЛЕКТРОННЫЙ ПРОМЕЖУТОЧНЫЙ АРХИВ DZAB

Источник: сайт Федерального архива Германии http://www.bundesarchiv.de/DE/Content/Artikel/Anbieten/Behoerden/Zwischenarchive/digitales-zwischenarchiv.html
Автор: Наташа Храмцовская

В последние годы кое-кто из коллег – особенно из ВНИИДАД – время от времени упоминал о федеральном **Электронном промежуточном архиве Германии (Digitales Zwischenarchiv des Bundes, DZAB)**, однако сколько-нибудь подробной информации о нём в свободно доступных источниках не было.

Имеющаяся информация о DZAB на русском языке

Мне удалось отыскать ряд материалов – это, например, посвященный DZAB абзац в статье Наталии Геннадиевны Суровцевой «Хранение электронных документов: Зарубежный опыт» в №4 журнала «Вестник культуры и искусств» за 2017 год (https://cyberleninka.ru/article/n/hranenie-elektronnyh-dokumentov-zarubezhnyy-opyt):

По этой причине в ФРГ для федеральных организаций создается Цифровой промежуточный архив. Внеофисное хранение документов, потерявших оперативное значение, освобождает административные системы по управлению электронными документами от вышедших из активного употребления документов и способствует более эффективной работе этой системы. Федеральные организации создают Пакет представления информации (ZIP), включая основные данные в сжатом файле и метаданные в файле на языке XML. Этот пакет посылается через безопасную сеть в Интерфейс доступа цифрового промежуточного архива. Затем Пакет представления информации преобразуется в пакет XAIP и метаданные извлекаются в базу данных для проведения исследований. После проверок и легализации пакет XAIP сохраняется, и федеральная организация получает его идентификацию. В 2015 г. было запланировано начало первой передачи данных и тестирование [6. с. 68-70].

Есть ещё опубликованный ВНИИДАД в 2013 году отчет о НИР «Проведение научных исследований в области комплектования, хранения, учета и использования архивных документов» в рамках подготовки «Обзора международного опыта организации временного хранения документов (промежуточных хранилищ)» (см. http://www.vniidad.ru/Downloads/ocnti/ОТЧЕТ%20НИР%20по%20контракту%202013.doc), в котором на стр.28 сказано:

«В соответствии с концепцией создания специализированного промежуточного архива электронных документов под эгидой Федерального архива предполагается расширение сферы предоставляемых федеральным

ведомствам информационных услуг в электронном виде. На основе хранимых в промежуточных архивах архивных материалов федеральных ведомств в электронном архиве будут созданы отраслевые банки электронных документов и электронные каталоги хранимых оцифрованных материалов.

В случае необходимости представители соответствующих ведомств получат возможность обращения к хранимым в банке данных своего ведомства электронным копиям документов для ознакомления с требующимися документами в режиме просмотра или скачивания. Программные средства электронного архива позволит обеспечить атрибутивный и полнотекстовый поиск хранящихся документов. При этом обеспечивается защита хранимых документов, строгое разграничение прав доступа в электронный архив.»

Наконец, о DZAB говорил Михаил Васильевич Ларин в своём докладе «Организация работы с электронными документами в Федеральном архиве Германии» на 3-ей Международной научно-практической конференции ИАИ РГГУ на тему «Документ. Архив. Информационное Общество», которая прошла в Пушкино 28-29 сентября 2017 года (см. https://books.google.ru/books?id=6ydaDwAAQBAJ):

«Политика правительства ФРГ направлена на сосредоточение информационных услуг федерального уровня в нескольких крупных федеральных информационных центрах. Один из таких центров находится в городе Нюрнберге и принадлежит Федеральной службе труда (занятости). Этот центр предлагает услуги по долгосрочному хранению документов для всех федеральных организаций, обеспечивая их безопасное хранение. На его базе и был создан Промежуточный архив электронных документов (DZaB). При этом все технологическое обеспечение процессов хранения электронных документов осуществляется Информационным центром службы труда, однако оперативное управление DZaB, т. е. всеми архивными функциями, является прерогативой Федерального архива. При таком подходе к решению вопроса достигается ряд преимуществ экономического, технологического, организационного свойства, а главное - обеспечивается своевременное и надежное хранение цифровых документов, чего невозможно было добиться при децентрализованном способе организации этой работы.

Инфраструктура Промежуточного архива электронных документов состоит из трех функциональных блоков:

- первый блок обеспечивает задачи приема в архив электронных документов и доступа к ним;
- второй блок обеспечивает защиту информации документов и средств шифрования документов, включая цифровую подпись;
- третий блок обеспечивает процессы хранения электронных документов и отбор их на постоянное хранение в Федеральном архиве.

Сам технологический процесс функционирования DZaB схематично можно представить следующим образом: электронные документы (ЭД) из систем по управлению электронными документами (ERDMS) министерств и ведомств поступают по информационно-коммуникационным сетям на хранение в Промежуточный архив. При этом создается так называемый пакет архивной

информации в формате XML (XAIP) в соответствии со стандартом безопасности TR-ESOR. В этот пакет включаются служебные и специальные метаданные, а также криптографические сведения, гарантирующие целостность и подлинность цифровой подписи, отметки времени и так далее. Пакет содержит также документ в оригинальном формате или в PDF/A.

Разработчики DZaB считают, что количество метаданных не должно превышать десяти позиций. Увеличение числа метаданных, по их мнению, повлечет за собой неоправданное усложнение системы. Поэтому в состав метаданных предлагается включить сведения: об идентификации пользователя (ID), название файла, наименование дела, представление версии, крайние даты, сроки хранения информации, описание, формат, ключевые слова. Важно отметить, что до проведения процедуры экспертизы ценности ЭД министерство или ведомство, передавшее документы в промежуточный архив, имеет право и возможность управлять своими документами: осуществлять их поиск, чтение, изменение, уничтожение. В то же время DZaB обязан обеспечить хранение, систематизацию, проверку аутентичности документов, а также возможность обратной конвертации ЭД из архивного пакета в системы ERDMS. DZaB включает в себя также специальные компьютерные модули, позволяющие эффективно обеспечить информационную безопасность массива архивных документов. После проведения экспертизы ценности отобранные на постоянное хранение ЭД передаются из Промежуточного архива в Федеральный архив для размещения в Цифровом архиве.

В настоящее время функционирование Промежуточного архива электронных документов происходит в тестовом (экспериментальном) режиме».

Результаты поиска информации

Недавно у меня появился мотив поискать информацию о данном архиве, и оказалось, что источников на немецком языке, в общем-то, тоже немного. Сегодня я хочу поделиться тем, что мне удалось «накопать».

Начну с того, что вступивший в силу в марте 2017 года Федеральный закон об архивах (Bundesarchivgesetz, BArchG, https://www.gesetze-im-internet.de/barchg_2017/ – у него есть и более длинное название: «Закон об использовании и защите федеральных архивных документов» – Gesetz über die Nutzung und Sicherung von Archivgut des Bundes) содержит отдельную статью 8 «Промежуточный архив и электронный промежуточный архив»:

1. Федеральный архив поддерживает промежуточный архив для неэлектронных документов высших федеральных органов власти и конституционных органов. Федеральный архив также поддерживает электронный промежуточный архив для электронных документов всех учреждений федерального правительства.

2. Федеральный архив хранит федеральные документы промежуточного архивного хранения от имени представившего их федерального государственного органа или преемника его прав и функций. До тех пор, пока эти документы не будут приняты на постоянное хранение как государственные

архивные документы, ответственность Федерального архива ограничивается необходимыми техническими и организационными мерами по сохранению и обеспечению безопасности документов. в соответствии с предложением 2 абзаца 2 ст.3 разрешается проведение Федеральным архивом предварительной экспертизы ценности промежуточных архивных активов федерального правительства; Абзац 5 ст.5 применяется с соответствующими поправками.

3. Передача электронных документов в электронный промежуточный архив должна проводиться в соответствии с обязательным стандартам, установленным для федеральной администрации. Если для формы передачи и для формата данных отсутствует обязательный стандарт для Федеральной администрации, то порядок передачи определяются по соглашению с передающим документы государственным органом.

На сайте Федерального архива Германии есть страница, посвященная Электронному промежуточному архиву, см. http://www.bundesarchiv.de/DE/Content/Artikel/Anbieten/Behoerden/Zwischenarchive/digitales-zwischenarchiv.html .

Она рассказывает следующее:

Рис. 1 – Электронный промежуточный архив

Федеральный архив (Bundesarchiv) предоставляет централизованное хранилище для долговременного защищённого хранения электронных документов.

В виде Электронного промежуточного архива Федеральный архив предоставляет всем подведомственным и независимым федеральным органам централизованное долговременное, соответствующее установленным требованиям хранилище для хранения имеющихся у них электронных документов.

Основной оказываемой DZAB услугой является услуги многоклиентской ИТ-системы хранения Федерального агентства занятости (Bundesagentur für Arbeit), которое имеет соответствующую инфраструктуру, многолетний опыт и, соответственно, высокий уровень обеспечения безопасности. Однако основной

точкой контакта для федеральных органов и судов остается Федеральный архив, который, таким образом, продолжает и расширяет проверенную опытом практику работы неэлектронных промежуточных архивов в условиях электронно-цифрового мира. Создание DZAB стало частью программы «Объединенная ИТ-инфраструктура федерального правительства» (Gemeinsame IT des Bundes), и, таким образом, DZAB вносит важный вклад в консолидацию ИТ на федеральном уровне.

Ваши преимущества от использования DZAB:

- Ваши потребности в хранении будут софинансироваться до 2019 года с учетом бюджетных потребностей;
- Ваши ИТ-системы систематически разгружаются;
- Ваши данные защищены и остаются доступными;
- Вы получаете новую личную, финансовую, техническую и организационную свободу;
- У Вас есть имеющее юридическую силу доказательство целостности, достоверности и полноты ваших данных;
- Вы быстро и легко выполняете свои обязанность предложить свои документы Федеральному архиву.

За дополнительной информацией страница отсылает к 14-страничному документу под названием «Информационная брошюра о подключении заинтересованных федеральных органов и судов к Электронному промежуточному архиву Германии» (Informationsbroschüre über die Anbindung interessierter Bundesbehörden und -gerichte an das Digitale Zwischenarchiv des Bundes (DZAB), см. http://www.bundesarchiv.de/DE/Content/Downloads/Anbieten/informationsbroschuere-anbindung-interessierter-bundesbehoerden-an-dzab.pdf?__blob=publicationFile), содержание которой следующее:

1. Введение
2. Правовые основы, инфраструктура и распределение обязанностей
3. Планируемый процесс электронного промежуточного архивирования
4. Расходы для органов, сдающих документы на хранение
5. Реализация подключения к DZAB

В брошюре разъясняется, что, согласно принятому в 2013 году «Законе об электронном правительстве» (Das Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften - E-Government-Gesetz, EGovG, http://www.gesetze-im-internet.de/egovg/), все федеральные органы власти и суды обязаны использовать электронные документы и обеспечить их хранение в соответствии с установленными требованиями. Самостоятельно выполнить эти требования в своих информационных системах для большинства органов дорого и сложно, и тогда они могут воспользоваться услугами Электронного промежуточного архива. Государственные органы сохраняют право собственности и доступ к своим документам, и, кроме того, им намного проще будет исполнить установленную законом обязанность предложить свои вышедшие из активного использования документы Федеральному архиву.

Процедуры промежуточного архивного хранения признаны соответствующими законодательству по защите персональных данных.

В основе DZAB лежит принадлежащее Федеральному агентству занятости решение SecDocs версии 3.0 (см. http://manuals.ts.fujitsu.com/file/12818/SecDocs.pdf), поставленное компанией Fujitsu Technology Solutions GmbH и разработанное специально с учетом требований немецких стандартов. Система обеспечивает долговременное хранение с защитой от внесения изменений и сохранением доказательной силы документов. Данные хранятся в двух высокодоступных системах хранения в Нюренберге – таким образом, обеспечивается хранение документов на территории Германии.

Ядро безопасности решения SecDocs сертифицировано на соответствие стандарту Common Criteria EAL4 и национальному Техническому руководству TR 03125 «Сохранение доказательной силы документов, подписанных с использованием криптографических методов» (Beweiswerterhaltung kryptoraphischsignierter Dokumente, TR-ESOR, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html) версии 1.2.

Система обеспечивает надёжное логическое разделение данных и метаданных, принадлежащих различным клиентам (физическое разделение ввиду сложности процессов и по экономическим причинам не реализуется). Все операции доступа, в т.ч. выполняемые администраторами, протоколируются. В любой момент ведомство-владелец может убедиться в аутентичности и целостности документов на основе подтверждающих документов (evidence records) в соответствии со спецификациями спецификации RFC 4998 ERS (от Evidence Record Syntax – *синтаксис документального свидетельства, представляющего собой структуру, поддерживающую долговременную неотказуемость от факта существования данных. Документ доступен по адресу* https://tools.ietf.org/html/rfc4998 – *Н.Х*.).

Для хранения электронных объектов используются самодокументированные архивные информационные пакеты в формате XML (XML-formatierten Archivinformationspakete, XAIP – см. рис. 2), описанные в спецификациях TR-ESOR – а именно, в документе под названием «Приложение F – Формат версии 1.2.1» (BSI TR-03125 Anlage TR-ESOR-F Formate Version 1.2.1, объёмом 51 страница, см. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_F_V1_2_1.pdf?__blob=publicationFile&v=2). Такие информационные пакеты представляют собой контейнеры, в которые упакован как контент, так и метаданные, необходимые для полного и надёжного восстановления всех соответствующих деловых и административных процессов на протяжении срока хранения. Этот же документ предписывает использовать для хранения контента только стандартизированные форматы, признанные пригодными для долговременного хранения. На сегодня в их число входят форматы простой текстовой (ASCII),

PDF/A-1, ODF для текстовых документов, TIFF, JPEG, PNG – для графических образов *(выбор, мягко говоря, небогатый – Н.Х.*).

Рис. 2 – Структура информационного пакета XAIP

Взаимоотношения сторон (показанные на рис. 3) устанавливаются административными соглашениями и соглашениями о качестве обслуживания.

Рис. 3 – Структура взаимодействия заинтересованных сторон

Передающие документы на хранение государственные органы отвечают за выполнение следующих задач:

- **Организация информационного обмена с Центром компетенции по вопросам промежуточной архивации Федерального архива.** Государственный орган назначает ответственного за промежуточную архивацию сотрудника (эта роль называется «Beauftragte/n für die Digitale Zwischenarchivierung», BfDZA), который становится единой точкой контакта по этим вопросам как для Центра компетенции, так и для структурных подразделений организации. Данный сотрудник отвечает за сбор всей

необходимой информации, имеющей отношение к промежуточному архивному хранению, обеспечивая своевременны обмен информацией и принятие окончательных решений.

- **Подготовка данных.** Передающий документы орган обеспечивает преобразование контента и метаданных в форматы долговременного хранения (сейчас это. соответственно, PDF/A и XML) и их совместную упаковку в информационный пакет. Кроме того, могут быть сохранены файлы в исходных форматах (например, в форматах Microsoft Office) и дополнительные метаданные. Таким образом, при желании возможно полное восстановление оригинальных документов.
- **Адаптация используемой государственным органом системы управлении документами.** Передающий орган отвечает за проведение необходимых для поддержки промежуточной архивации доработок своей системы (например, создание интерфейса экспорта-импорта).
- **Организация первичной технической поддержки** своих сотрудников.
- **Оценка требуемых ресурсов и оплата счетов.** Передающий орган обязан уведомлять DZAB об объёмах хранения на предстоящий финансовый год. Он также обязан проверить и оплатить выставляемые Федеральным архивом счета.
- **Адаптация политики безопасности и защиты персональных данных.** Передающий орган обязан адаптировать свои внутренние политики таким образом, чтобы сделать возможным использование DZAB.

Центр компетенции в сфере промежуточной архивации отвечает за выполнение следующих задач:

- Специальное и техническое консультирование передающего документы государственного органа;
- Разработка интерфейсов к электронному промежуточному архиву;
- Техническая поддержка второго уровня;
- Решение административных и координационных задач;
- Передача отобранных на постоянное хранение данных в электронное хранилище (Digitale Magazin des Bundesarchivs) Федерального архива (сюда входит реализация функциональных возможностей, поддерживающих экспертизу ценности в Электронном промежуточном архиве и организация процесса передачи в электронное хранилище Федерального архива;
- Отдельный компонент доступа, через который по умолчанию осуществляется доступ к заархивированным данным.

Состояние проекта DZAB

В опубликованном в мае 2017 года отчете для Бундестага о ходе выполнения программы «Электронное правительство 2020» отмечалось, что проект пока находится в пилотной фазе, в нём участвует 4 партнера и ещё 3 стороны заявили о желании присоединиться к проекту в 2017 году. Партнеры проекта также в этот момент частично занимались внедрением, а частично ещё были на стадии проведения закупок.

По итогам проведенного опроса более половины (55.4%) респондентов собирались использовать услуги Электронного промежуточного архива Германии.

Дополнительная литература

Михаэль Ухарим (Michael Ucharim) «Электронный промежуточный архив Германии» (Das Digitale Zwischenarchiv des Bundes), журнал Scrinium Ассоциации австрийских архивистов (Verband Österreichischer Archivarinnen und Archivare, VÖA), том 69, 2015 год, стр. 137-145, http://www.voea.at/tl_files/content/Scrinium/Scrinium%2069/Scrinium_69_137-145.pdf

Sandro Hardy, Rainer Jacobs, Dr Michael Ucharim «Электронный промежуточный архив Германии: Централизованное хранилище для федеральных органов власти и судов» (Das Digitale Zwischenarchiv des Bundes - Die zentrale Speicherlösung für Bundesverwaltung und Bundesgerichte), Behördenforum 2018 Koblenz, 16 Januar 2018, Berlin, 18 Januar 2018 (презентация), http://www.bundesarchiv.de/DE/Content/Downloads/Anbieten/informationsforum-2018-praesentationen-hardy.pdf?__blob=publicationFile

Dr Sebastian Gleixner, Dr Michael Ucharim «Электронный промежуточный архив Германии: Централизованное хранилище для федеральных органов власти и судов» (Das Digitale Zwischenarchiv des Bundes - Die zentrale Speicherlösung für Bundesverwaltung und Bundesgerichte), Frankfurt, 13 Oktober 2016 (презентация), http://www.langzeitarchivierung.de/Subsites/nestor/SharedDocs/Downloads/praesentationen/2016NewbiesII-GleixnerBarch.pdf?__blob=publicationFile

Michael Ucharim, Thomas Seliger «Электронный промежуточный архив Германии: Централизованное хранилище для федеральных органов власти» (Das Digitale Zwischenarchiv des Bundes - Die zentrale Speicherlösung für Bundesverwaltung), Berlin, 19-20 November 2014 (презентация), https://www.infora-mc.de/Das-Digitale-Zwischenarchiv-des-Bundes-Zentrale-Speicherloesung-fuer-die-Bundesverwaltung-870445.pdf

Michael Ucharim «Электронный промежуточный архив Германии» (Das Digitale Zwischenarchiv des Bundes), Koblenz, 14 Januar 2014 (презентация), http://www.bundesarchiv.de/imperia/md/content/abteilungen/abtb/bbea/vortrag_ucharim.pdf

Michael Ucharim «Электронный промежуточный архив Германии: Концепция и текущее положение дел» (Das Digitale Zwischenarchiv des Bundes – Konzeption und aktueller Stand der Umsetzung), 18 Arbeitstagung des Arbeitskreises «Archivierung von Unterlagen aus digitalen Systemen», Weimar, 11-12 März 2014 (презентация), https://www.staatsarchiv.sg.ch/home/auds/18/_jcr_content/Par/downloadlist_0/DownloadListPar/download_1.ocFile/Praesentation%20Ucharim.pdf

Dr. Michael Hollmann «Электронный промежуточный архив Федерального архива как общая служба для государственных органов» (Das digitale Zwischenarchiv beim Bundesarchiv als Shared Service für die Bundesverwaltung),

13. Mai 2009 (презентация), https://www.bundesarchiv.de/imperia/md/content/abteilungen/abtb/bbea/01_hollmann__digzwarch_2009-05-13.pdf

«Принципы федеральной ИТ-архитектуры» (Architekturrichtlinie für die IT des Bundes), редакция 2017 года – см. DAAV-09: «Использование услуг Электронного промежуточного архива Германии» (Nutzung des Dienstes Digitales Zwischenarchiv des Bundes) на стр. 56, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/IT-Konsolidierung/architekturrichtlinie_itbund.pdf?__blob=publicationFile

«Информация федерального правительства о ходе программы «Электронное правительство 2020»: Оценка по состоянию на 2016 год» (Unterrichtung durch die Bundesregierung: Digitale Verwaltung 2020 – Evaluierungsbericht 2016), Бундестаг Германии, 19.05.2017, см. раздел 4.9, http://dip21.bundestag.de/dip21/btd/18/125/1812512.pdf

ВОПРОС КОЛЛЕГИ: С ЧЕГО НАЧИНАТЬ СОЗДАНИЕ ЭЛЕКТРОННОГО АРХИВА?

Автор: Наташа Храмцовская

Вопрос: *Прошу Вас поделиться имеющимся опытом, а также, при наличии такой возможности, посоветовать конкретные шаги по реализации электронного архива (с чего начать, к кому обратиться за консультацией, какие действия необходимо предусмотреть и т.д.)?*

Ответ: Первое, что нужно – это создать команду проекта, в которую должны войти различные специалисты Вашей организации, отвечающие за работу с информацией и документацией.

Они должны разработать план реализации проекта, куда могут войти задачи:

- Формирование функциональных требований к информационной системе электронного архива;
- Проведение экспертизы документации организации и её оценки на предмет возможности перевода в электронный вид;
- Оценка потребностей использования различных видов электронных подписей для документации.

После того, как Вы проведёте эту работу, Вам станет ясно, в каком направлении Вам нужно развивать Ваш электронный архив, и какие документы в первую очередь стоит переводить в электронный вид.

Много дополнительной информации Вы сможете найти на моем блоге http://rusrim.blogspot.ru/, особенно если освоите использование поиска по блогу (поле слева, под фотографиями) и тегов (большая колонка слева внизу).

Понятно, что там нет готового плана создания электронного архива в коммерческой организации, но материалов там много и разных, и для освоения различных вопросов электронной архивации они могут Вам пригодится.

У меня есть богатая коллекция видеозаписей докладов в т.ч. по электронным архивам (не только моих) – см. https://www.youtube.com/channel/UC8KrhYA3LREYZCq_16qiYyA/videos .

Вы можете посмотреть коллекцию моих презентаций https://www.slideshare.net/sspchram/presentations/ (к сожалению, сейчас для доступа к ней Вам понадобиться анонимайзер) – там есть несколько презентаций по тематике электронных архивов.

Ещё один способ получить информацию – личное участие в различных рода конференциях, где в кулуарах можно обменяться опытом и обсудить проблемы с коллегами из других коммерческих организаций.

ВОПРОС КОЛЛЕГИ: ОТКАЗ ОТ ДОКУМЕНТОВ НА БУМАЖНЫХ НОСИТЕЛЯХ

Автор: Наташа Храмцовская

Вопрос: *Наша организация рассматривает вопрос об отказе бумажного варианта эксплуатационной и распорядительной документации, оставив исключительно электронный формат. В РФ такая практика отсутствует, но на конференции в Казани в апреле 2018 гола было озвучено, что данный опыт имеется во Франции и в Канаде. Не могли бы Вы подсказать, где можно более подробно с ним познакомиться.*

Ответ: Практика отказа от бумаги есть и в России – во всяком случае, ряд крупных коммерческих организаций очень активно идёт по этому пути. Некоторые документы в принципе уже не могут быть полноценным образом представлены на бумаге, особенно если дело касается чертежей. Иное дело, что перевести исключительно в электронный вид все и сразу ни у кого не получается.

Вы назвали две группы документов – эксплуатационная и распорядительная документация. Как Вы сами понимаете, назначение этих групп очень разное, более того, для перевода их в электронный вид требуется проведение серьезной экспертной работы, оценки рисков и т.д. Особенно это касается эксплуатационной документации.

Опыт Франции и Канады – это главным образом опыт хранения организационно-распорядительной, бухгалтерской и налоговой документации,

других деловых документов. Ключевым элементом там является сертификация соответствующих систем хранения на соответствие национальным стандартам, и в этом случае законодательство дает хранимым в таких системах электронным документам презумпцию подлинности. У нас, к сожалению, нет ни стандартов такого рода, ни законодательных норм. Из этого опыта можно взять ряд хороших требований к системам хранения электронных документов. Если говорить конкретно, то **во Франции** это стандарты:

1) **NF Z 42-013:2009 «Электронная архивация – Требования к разработке и использованию информационных систем по обеспечению сохранности и целостности содержащихся в этих системах документов»** (Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes, см. https://www.boutique.afnor.org/norme/nf-z42-013/archivage-electronique-specifications-relatives-a-la-conception-et-a-l-exploitation-de-systemes-informatiques-en-vue-d-assurer/article/773362/fa125098).

На основе этого стандарта был подготовлен международный стандарт **ISO 14641-1:2012** «Управление электронными документами – Часть 1: Требования к проектированию и эксплуатации информационных систем для обеспечения долговременной сохранности электронной информации» (Electronic archiving – Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation) – сейчас он пересматривается и скоро выйдет новая редакция.

См. посты на моем блоге:

- Стандартизация во Франции: NF Z 42-013 - NF Z 42-020 - NF Z 42-025 – что дальше?, https://rusrim.blogspot.com/2012/07/nf-z-42-013-nf-z-42-020-nf-z-42-025.html .
- Выигрышное уравнение электронной архивации: NF Z 42-013 + ISO = ISO 14641-1, https://rusrim.blogspot.com/2011/07/nf-z-42-013-iso-iso-14641-1.html .
- Франция: Началась работа по пересмотру стандарта NF Z 42-013 «Электронная архивация – Требования к разработке и использованию информационных систем по обеспечению сохранности и целостности содержащихся в этих системах документов», https://rusrim.blogspot.com/2015/10/nf-z-42-013.html .
- Франция: Как идёт пересмотр стандарта NF Z 42-013?, https://rusrim.blogspot.com/2017/10/nf-z-42-013.html .
- Международная организация по стандартизации утвердила новый стандарт по обеспечению сохранности электронных документов, https://rusrim.blogspot.com/2012/01/blog-post_5411.html .

2) **NF Z 42-020:2012 «Функциональные характеристики компоненты «Электронный сейф», предназначенной для сохранения электронной информации в условиях, обеспечивающих её целостность во времени»** (Spécifications fonctionnelles d’un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps), см. https://www.boutique.afnor.org/norme/nf-z42-

020/specifications-fonctionnelles-d-un-composant-coffre-fort-numerique-destine-a-la-conservation-d-informations-numeriques-dans-des-/article/796213/fa176610 . Сейчас в ИСО рассматривается вопрос о создании на основе этого документа международного стандарта.

См. посты на моем блоге:

- Франция: Регулятор сформулировал свою позицию в отношении услуг «электронного сейфа» – как теперь относиться к стандарту NF Z 42-020?, https://rusrim.blogspot.com/2013/10/nf-z-42-020.html .
- Франция: Новый стандарт «электронного сейфа» NF Z 42-020, https://rusrim.blogspot.com/2012/03/nf-z-42-020.html .

3) Дополняет предыдущие два документа стандарт **NF Z 42-026 «Определение и спецификации услуг по надёжной оцифровке документов на бумажном носителе и контроль над оказанием этих услуг»** (Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations, https://www.boutique.afnor.org/norme/pr-nf-z42-026/definition-et-specifications-des-prestations-de-numerisation-fidele-de-documents-et-controle-de-ces-prestations/article/874692/fa187367).

См. пост на моем блоге «Надежная оцифровка и уничтожение оригиналов: Наступил ли конец бумаги?», https://rusrim.blogspot.com/2017/09/blog-post_14.html .

В Канаде – это стандарт **CAN/CGSB-72.34-2017 «Электронные документы как документальное доказательство»** (Electronic Records as Documentary Evidence), https://www.scc.ca/en/standardsdb/standards/28933 .

См. пост на моем блоге «Канада: Опубликована новая редакция стандарта CAN/CGSB 72.34-2017 «Электронные документы как документальные доказательства»», https://rusrim.blogspot.com/2017/05/cancgsb-7234-2017.html

ИЗУЧЕНИЕ ПРОБЛЕМЫ ПОДТВЕРЖДЕНИЯ АУТЕНТИЧНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ: ПЕРВЫЕ РЕЗУЛЬТАТЫ ПРОВЕДЕННОГО ИССЛЕДОВАНИЯ

Источники: 1. Сайт Федерального агентства, http://archives.ru/reporting/report-artizov-2018-sovet.shtml

2. Luciana Duranti «Concepts and principles for the management of electronic records, or records management theory is archival diplomatics», Records Management Journal, Vol. 9 No. 3, pp. 149-171 (1999); статья была переопубликована в том же журнале в 2010 году, Vol. 20 No. 1, pp. 78 – 95, см. https://www.academia.edu/11327974/Concepts_and_principles_for_the_management_of_electronic_records_or_records_management_theory_is_archival_diplomatics

3. Corinne Rogers Virtual authenticity: Authenticity of digital records from theory to practice, PhD Thesis, University of British Columbia, Vancouver, 2015, https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0166169
Автор: Наташа Храмцовская

В докладе Руководителя Федерального архивного агентства Андрея Николаевича Артизова на торжественном заседании Совета по архивному делу при Федеральном архивном агентстве, посвящённому 100-летию государственной архивной службы России 1 июня 2018 года, было отмечено, что подтверждение аутентичности электронного документа является отдельной проблемой, которую архивной отрасли предстоит решать наряду с другими проблемами и задачами (см.: http://archives.ru/reporting/report-artizov-2018-sovet.shtml).

Так уж получилось, что в 2017 году в рамках одного консалтингового проекта мне пришлось изучать вопросы теории аутентичности на основе выявленных в открытом доступе научных работ зарубежных и российских исследователей, а также международных и российских стандартов, в которых в той или иной степени затрагиваются вопросы обеспечения аутентичности документов, в том числе и электронных.

Анализ выявленных стандартов и литературы показал, что в первую очередь исследования посвящены следующим вопросам:

- Наибольшее внимание в работах уделяется определению понятия аутентичности; в меньшей степени рассматривается вопрос о различии между аутентичностью и подлинностью электронных документов;
- Значительно меньше работ посвящено вопросам роли аутентичности и методам ее обеспечения (техническим и нетехническим), в том числе таким темам, как потребности в сохранении аутентичности документов, особенности обеспечения аутентичности электронных документов, принципы и способы установления и обеспечения аутентичности.

Ведущий мировой специалист в области дипломатики и теории современного управления документами и архивного дела Лючиана Дюранти (Luciana Duranti), говоря о значимости вопроса аутентичности в эпоху активного использования электронных документов, в своей статье «Концепции и принципы управления электронными документами, или: теорией управления документами является архивная дипломатика» подчеркивает:

«Наибольшие проблемы из тех, что ставят перед нами электронные системы, – это создание и поддержание надежных документов и сохранение их аутентичности с течением времени. Для каждой организации жизненно важно, чтобы её документы были в состоянии подтверждать факты, к которым они относятся, т.е. чтобы содержание этих документов заслуживало доверия. Для решения этих проблем международному сообществу специалистов по управлению документами необходимо разработать соответствующие стратегии, процедуры и стандарты.» (см.: https://www.academia.edu/11327974/Concepts_and_principles_for_the_management_of_electronic_records_or_records_management_theory_is_archival_diplomatics .

Её коллега Коринн Роджерс (Corinne Rogers) в своей работе отмечает: «Традиционная архивная модель аутентичности документов, опирающаяся на установление идентичности и демонстрацию целостности, по-прежнему может рассматриваться в качестве фундамента для аутентичности документов в электронной среде, однако, она требует расширения и/или адаптации с тем, чтобы учесть проблемы, связанные с электронными технологиями. Проблема аутентичности в электронной среде является в такой же степени социальной, как и технической. Решения проблемы установления и защиты аутентичности разнообразны и неупорядочены. В одних случаях может быть целесообразно использовать технические и процедурные меры и средства контроля и управления, в то время как в других может быть достаточным или даже единственно возможным применение «человеческих» и социальных средств.» (см.: https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0166169).

На основе изучения и анализа выявленных материалов в отчете было сделано следующее:

- Проведен анализ существующей на настоящий момент теории аутентичности в области делопроизводства и архивного дела;
- Обобщены вопросы организации хранения электронных документов в случае утраты аутентичности и (или) целостности документа;
- Дана оценка роли аутентичности и описаны методы ее обеспечения (технические и нетехнические);
- Выявлены и описаны проблемы обеспечения аутентичности электронных документов при их долговременном хранении
- Даны рекомендации по обеспечению аутентичности и доверия к электронным документам и информации

США: НОВЫЕ ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ЭЛЕКТРОННОЙ ПОЧТЫ И ИХ ПОСЛЕДСТВИЯ ДЛЯ УПРАВЛЕНИЯ ДОКУМЕНТАМИ

Источник: блог Национальных Архивов США https://records-express.blogs.archives.gov/2018/05/23/email-system-features-and-records-management/

Автор: Ариан Раванбакш

В течение последних нескольких недель был опубликован ряд статей, описывающих предстоящие изменения, которые Google в настоящее время развёртывает в своём почтовом сервисе. Одна из этих функциональных возможностей, так называемый «конфиденциальный режим» (confidential mode), позволяет отправителям устанавливать, в течение какого периода

времени получатель сможет читать и получать доступ к сообщениям; блокировать возможность пересылки или копирования/вставки; а также установить, когда сообщение будет удалено. В Национальные Архивы США поступили вопросы о том, какие будут иметь последствия этих возможностей для управления документами.

Во-первых, независимо от того, какую платформу федеральный орган исполнительной власти выбирает для своей электронной почты, он несёт ответственность за обеспечение соблюдения всех требований и указаний по вопросам управления документами, которые содержатся в федеральном законодательстве и в нормативных актах, выпущенных Национальными Архивами. Сюда входит применение на практике и отслеживание сроков хранения, установленных соответствующими, одобренными Национальными Архивами перечнями документов с указанием сроков хранения. Все решения о разрешении использования определенных функций или функциональных возможностей платформы электронной почты будет приниматься самими государственными органами. Эти решения, однако, должны также соответствовать всем соответствующим законам и нормативным актам. Федеральные органы исполнительной власти должны тщательно оценивать новые функциональные возможности и технологии, прежде чем допустить их использование.

На протяжении ряда лет мы постоянно выпускали рекомендации для федеральных органов, подчеркивая их обязанность обеспечить надлежащее управление документами в электронной почте. В числе этих рекомендаций Бюллетень NARA 2014-06 «Руководство по управлению электронной почтой» (Guidance on Managing Email, https://www.archives.gov/records-mgmt/bulletins/2014/2014-06.html, *см. также пост* https://rusrim.blogspot.ru/2015/05/2_19.html) и Бюллетень NARA 2013-03 «Рекомендации для сотрудников федеральных органов исполнительной власти по управлению федеральными документами, в том числе учетными записями электронной почты, и по защите федеральных документов от неавторизованного изъятия» (Guidance for agency employees on the management of Federal records, including email accounts, and the protection of Federal records from unauthorized removal, https://www.archives.gov/records-mgmt/bulletins/2013/2013-03.html, *о нём см. также* https://rusrim.blogspot.ru/2013/10/blog-post_1.html).

Мы также опубликовали «Критерии управления документами в электронной почте в соответствии с Директивой по управлению государственными документами M-12-18» (Criteria for Managing Email Records in Compliance with the Managing Government Records Directive M-12-18, https://www.archives.gov/records-mgmt/email-management/2016-email-mgmt-success-criteria.pdf, *о них см. также* https://rusrim.blogspot.ru/2016/04/blog-post_36.html), позволяющие органам исполнительной власти оценить, в какой степени они обеспечивают управление электронной почтой в соответствии с Директивой по управлению государственными документами (OMB M-12-18,

https://www.archives.gov/records-mgmt/m-12-18.pdf, *о ней см. также* http://rusrim.blogspot.ru/2012/08/i_27.html).

В настоящий момент пока что неясно, когда будет – и будет ли вообще – «конфиденциальный режим» электронной почты Google доступен в почтовых системах федеральных органов исполнительной власти, однако перечисленные выше требования к управлению и обеспечению долговременной сохранности электронных сообщений будут по-прежнему применимы, и мы будем ожидать от федеральных органов их соблюдения.

Мы продолжим следить за новыми техническими разработками и, при необходимости, публиковать разъяснения и рекомендации.

ДОКУМЕНТАЦИОННЫЙ АНАЛИЗ – ПРОЦЕСС УСТАНОВЛЕНИЯ ТРЕБОВАНИЙ К ЗАХВАТУ И СРОКАМ ХРАНЕНИЯ ДОКУМЕНТОВ

Источник: сайт PROV https://www.prov.vic.gov.au/recordkeeping-government/a-z-topics/appraisal

Автор: Наташа Храмцовская

Сегодня я хочу предложить вниманию читателей перевод страницы сайта Управления государственных документов австралийского штата Виктории документов (Public Record Office Victoria, PROV), посвященной документационному анализу (appraisal), под которым понимается регулярно проводимый анализ деловых процессов организации в плане управления документами, в том числе с целью принятия решений о том, какие документы и системы, и в какой форме вообще следует создавать. Страница последний раз обновлялась 17 мая 2018 года.

Мой комментарий: *Любопытно видеть, как сами австралийские специалисты, во всем мире продвигающие «документационный анализ», постоянно сбиваются с новой трактовки соответствующего англоязычного термина appraisal на более узкую традиционную – экспертизу ценности документов).*

Что такое документационный анализ?

Документационный анализ – это процесс оценки деловых функций и операций с целью определить:

- Какие документы необходимо создавать и захватывать;
- В течение каких сроков следует хранить документы с тем, чтобы удовлетворить деловые потребности, обеспечить подотчетность организации и соответствовать ожиданиям общественности (адаптировано из публикации Bettington, J. et al. (eds) 2008, Keeping archives, 3rd edn, Australian Society of Archivists, Canberra pp. 11-28.);

Концепция документационного анализа PROV

Текущие усилия Управления государственных документов штата Виктория (PROV) в области документационного анализа соответствуют современной австралийской практики – обращается особое внимание на контекстуальную ценность документов посредством оценки в первую очередь функций и видов деятельности, а не собственно документов.

Соответствующая политика и принятые по результатам экспертизы ценности решения в отношении документов государственных органов исполнительной власти штата Виктория приведены в следующих документах:

- «Политика проведения экспертизы ценности и отбора государственных документов штата на архивное хранение» (Appraisal Statement for Public Records required as State Archives Policy, https://www.prov.vic.gov.au/recordkeeping-government/document-library/appraisal-statement-policy, прямая ссылка https://www.prov.vic.gov.au/sites/default/files/2016-05/Appraisal-Statement-for-State-Archives-Web.pdf);
- «Указания по срокам хранения и действиям по их истечении» (Retention and Disposal Authorities, RDAs, см. https://www.prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas – *это стандарты PROV, утвержденные руководителем архивно-документационной службы штата и являющиеся нормативными документами, авторизующими уничтожение либо передачу на постоянное архивное хранение государственных документов – Н.Х.*);
- Сводные отчеты о проведении экспертизы ценности (Summary Appraisal Reports, примеры будут выложены позже).

Экспертиза ценности с целью установления сроков хранения

В общем случае по итогам экспертизы ценности может быть принято решение о том, что документы имеют:

- Постоянную ценность как государственные архивные документы;
- Временную ценность, т.е. такие документы нужны лишь в течение определенного периода времени.

Ниже приводится в общих чертах схема подхода к проведению экспертизы ценности с целью установления документам сроков хранения с учетом деловых потребностей в них и их возможной постоянной ценности как государственных архивных документов.

Понимание и применение критериев экспертизы ценности имеет важное значение для:

- Приоритизации выделяемых на управление документами ресурсов и смягчения рисков. Дополнительную информацию см. на странице «Документы высокой ценности и риска – введение» (High value, high risk introduction, https://www.prov.vic.gov.au/recordkeeping-government/a-z-topics/high-value-high-risk-introduction);
- Разработки указаний по срокам хранения и действиям по их истечении. Дополнительную информацию см. на странице «Разработка

указаний по срокам хранения шаг за шагом» (RDA development step-by-step, https://www.prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/rda-development-step-by-step).

Экспертиза ценности документов временного срока хранения на основе законодательно-нормативных, организационных и деловых требований

Критерии:

- Законодательно-нормативные требования и требования политик;
- Обеспечение подотчетности;
- Роль в подтверждении и защите прав и привилегий;
- Роль в процессах принятия решений и административного управления;
- Роль документов как корпоративной памяти государственного органа.

Экспертиза ценности документов постоянного срока хранения (государственных архивных документов)

Критерии:

- Полномочия, миссия и структура;
- Основные функции и программы;
- Долговременные права и привилегии;
- Значительные последствия для отдельных лиц;
- Управление окружающей средой и соответствующие изменения;

- Значительный вклад в культурно-историческую память общества.

Мой комментарий: *Все перечисленные критерии на сайте раскрываются более детально при переходе по соответствующим гиперссылкам.*

ПРОБЛЕМЫ ХРАНЕНИЯ ЭЛЕКТРОННЫХ НАУЧНО-ТЕХНИЧЕСКИХ ДОКУМЕНТОВ

Источник: Youtubehttps://www.youtube.com/watch?v=pOYO6ZPwjrI
Автор: Наташа Храмцовская

На Международной научно-практической конференции «От пергамена к цифре», которая прошла в Казани 18 – 19 апреля 2018 года, одновременно с круглыми столами в соседнем зале шли доклады.

Один очень интересный и важный по своей проблематике доклад «Проблемы хранения электронных научно-технических документов» представил заместитель директора Российского государственного архива научно-технической документации (РГАНТД) Павел Алексеевич Кюнг.

Отмечу, что РГАНТД – единственный государственный архив нашей страны с поливидовым составом документов по истории отечественной истории науки и техники. Он хранит уникальные электронные документы с 1974 года, с момента своего создания, и у него накоплен огромный практический опыт обеспечения долговременной сохранности электронной научной документации и данных.

Специалисты архива внимательно изучают текущие проблемы электронных научно-технических документов, – и именно этому и был посвящен данный доклад.

https://youtu.be/pOYO6ZPwjrI
https://youtu.be/pOYO6ZPwjrI?t=9

НОВЫЙ БРИТАНСКИЙ СТАНДАРТ BS 10754-1:2018 ОБЕСПЕЧЕНИЯ ДОВЕРИЯ К СИСТЕМАМ, ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ И УСЛУГАМ

Источник: сайт Британского института стандартов https://shop.bsigroup.com/ProductDetail?pid=000000000030351844

В феврале 2018 года Британский институт стандартов (BSI) опубликовал интересный национальной стандарт **BS 10754-1:2018 «Информационные технологии. Доверие к системам. Требования к стратегическому и оперативному управлению»** (Information technology. Systems trustworthiness. Governance and management specification), см. https://shop.bsigroup.com/ProductDetail?pid=000000000030351844

Здесь стоит отметить, что тема доверия к электронным документам и информации, а также к поддерживающим их инфраструктуре и технологиям в последнее время стала очень популярной. В данном стандарте заслуживающим доверия считают объект (см. п.3.29), который «надлежащим образом решает вопросы защищённости и безопасности, надёжности, готовности к работе и живучести».

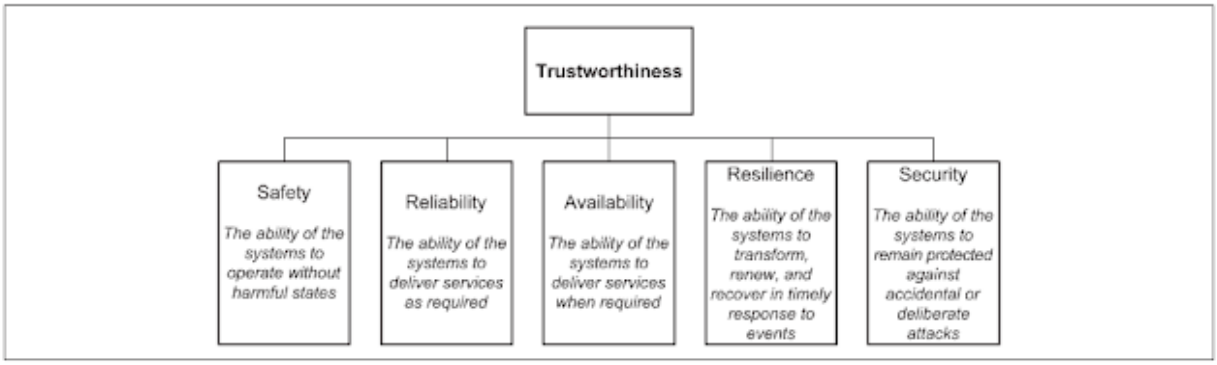
Как отмечается в документе, задача стандарта – способствовать повышению доверия к системам, программному обеспечению и услугам. Данный британский стандарт содержит требования и рекомендации по обеспечению доверия к системам, программному обеспечению и услугам, которая призваны стать широко используемым подходом, который может быть настроен с учетом специфических особенностей любой организации и программного обеспечения.

Требования данного стандарта определяют общие принципы эффективного обеспечения доверия и включают технические, физические, культурные и поведенческие меры, равно как и эффективное руководство и стратегическое управление. В нём описаны необходимые инструменты, методы

и процессы, а также рассмотрены вопросы защиты, надежности, готовности к работе, доступность, живучести и безопасности.

При этом стандарт детально не регламентирует те процессы или действия, которые организация применяет для достижения соответствующих результатов. Эти процессы описаны в иных стандартах и могут быть установлены самой организацией.

Figure *1 — Facets of trustworthiness*



В стандарте пятью ключевыми аспектами доверия (trustworthiness) считаются безопасность (safety), надёжность (reliability), готовность к работе (availability), живучесть/устойчивость (resilience) и защищённость (security).

Стандарт включает в себя всеохватывающую «Концепцию системы обеспечения доверия» (Trustworthiness System Framework, TSFr), которая представляет собой нейтральный в отношении сферы применения и способа реализации подход к использованию существующего большого объема знаний, включая вопросы защищённого функционирования, информационной безопасности, а также проектирования систем и программного обеспечения. Концепция «работает» как свод хорошей практики по обеспечению доверия к программному обеспечению.

Стандарт может применяться любыми организациями, стремящимися внедрить у себя практику обеспечения доверия к системам. Его могут использовать представители всех трёх основных сегментов ИТ-отрасли, а именно:

- Те, кто устанавливает требования (сфера закупок / приобретения);
- Те, кто реализует решения (разработчики и системные интеграторы);
- Конечные пользователи программного обеспечения.

Применение данного стандарта поможет организациям улучшить:

- Меры и средства контроля и управления;
- Эффективность и продуктивность оперативной деятельности;
- Обучение в организации;
- Уверенность и доверие заинтересованных сторон;
- Управление рисками;

- Деловую репутацию;
- Вероятность достижения организацией своих целей.

Способствуя увеличению доверия к программному обеспечению, стандарт может способствовать получению значительной экономии в рамках национальной экономики, а также снизить для ряда отраслей риск крупномасштабных чрезвычайных ситуаций.

Содержание стандарта следующее:

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Контекст
5. Метод
6. Реализация на практике

Приложение A (нормативное): Ключевые меры обеспечения доверия

Приложение B (справочное): Взаимосвязь мер BS 10754-1 с действиями по обеспечению доверия (Trustworthiness Activities, TA) в рамках жизненного цикла системы

Приложение C (справочное): Нефункциональные требования

Приложение D (справочное): Архетипы ИТ-систем

Библиография

В настоящее время идёт работа над другими частями стандарта:

- Часть 2: Варианты обеспечения уверенности (Assurance cases);
- Часть 3: Меры и средства обеспечения безопасности приложений (Application security controls).

Для специалистов по управлению документами вопрос доверия к системам становится актуальным, поскольку всё чаще одним из условий доверия к электронным документам, хранимым в ИТ-системах, является как раз доверие к самим этим системам. В ряде стран такая идея уже отражена в нормативно-правовой базе, регламентирующей работу судебной системы и процессы представления доказательств.

ЭЛЕКТРОННАЯ АРХИВАЦИЯ: «КОНТЕКСТ – ЭТО НАШЕ ВСЁ»

Источник: Блог Национальных Архивов Великобритании http://blog.nationalarchives.gov.uk/blog/digital-archiving-context-everything/
Автор: Джон Шеридан

В чём разница между архивом и хранилищем данных? Чем электронные архивы отличаются от других коллекций данных?

Возможно, самым важным отличием является интеллектуальный контроль (intellectual control), который для нас является одной из самых важных целей. Архив не только знает, какую информацию он хранит, но также **располагает ключевыми знаниями об этих активах**. Контекст каждого документа крайне важен для понимания как его исторической ценности, так и ценности в качестве юридического доказательства. Говоря словами известного социолога Элвина Уорда Гоулднера (Alvin Ward Gouldner), «Контекст – это наше всё».

Что значит иметь интеллектуальный контроль над электронным архивом? Наша «Электронная стратегия» (Digital Strategy, http://www.nationalarchives.gov.uk/about/our-role/plans-policies-performance-and-projects/our-plans/digital-strategy/) объясняет, что существует четыре вида полезности электронного архива для его пользователей: обеспечение долговременной сохранности, обеспечение взаимосвязи с контекстом (контекстуализация), представление и обеспечение возможностей для использования. Никакое другое учреждение не уделяет такое внимание контекстуализации своих материалов, как архив. Предоставление контекста – это наша архивная суперсила, придающая ценность информации, которая в противном случае была бы случайной, не прошедшей проверку на аутентичность.

Внутри электронной библиотеки на современных магнитных лентах

Традиционно существовало ключевое различие между историческим и архивным контекстами. Понимание исторического контекста документа заключается в знаниях о том, что происходило во время его создания; о том, как те события, которые он описывает или уточняет, вписываются в хронологическую последовательность событий. С точки зрения архива, это была задача историка - помочь Вам увидеть картину событий в целом, чтобы Вы могли понять, как в неё вписывается Ваша деталь головоломки.

Архивист может интересоваться историческим контекстом, но, по большому счёту, мы всегда считали, что его предоставление в задачи архива не

входит. Наша задача заключалась в том, чтобы помочь пользователю документа в достаточной мере понять контекст его создания и использования, чтобы иметь возможность оценить его доказательную ценность. Кто его создал и каковы были роли этих лиц? Какое влияние и значение имел этот человек или учреждение? При каких обстоятельствах был создан документ, и с какой целью? Почему он был отобран на постоянное архивное хранение? Как история его ответственного хранения влияет на его ценность?

Это была та ключевая информация, которой архив обладал и которую он должен был выдавать пользователям документов. Мы всегда это делали посредством архивного каталога, основного инструмента для получения доступа к нашим документам – в каталоге содержатся сведения об информации, которые необходимы пользователям для её правильного понимания.

Электронные документы предъявляют к нам новые требования в том, что касается установления интеллектуального контроля над коллекцией:

Электронная стратегия Национальных Архивов Великобритании на 2017 – 2019 годы

«Мы переосмыслим наш подход к описанию и контекстуализации электронных документов. Нам необходимо внедрить совершенно новый подход к описанию документов, основанный на потребностях пользователей... Нам нужно изучить возможности разрыва жесткой связи между отдельными документами и описанием, и попытаться найти более гибкие подходы».

Нам нужно переосмыслить то, как мы предоставляем сведения о контексте. Описания контекста какого рода мы должны предоставить пользователям наших электронных документов? Какие метаданные нам нужно собрать у людей, которые создают электронные документы, в тот момент, когда эти документы поступают в архив? Насколько много деталей нам следует установить и зафиксировать самостоятельно путем обработки этих документов, с тем, чтобы обогатить описания и контекстуализировать документы?

Мы опубликовали документ с изложением нашей позиции (http://www.nationalarchives.gov.uk/about/our-role/plans-policies-performance-and-projects/our-plans/our-digital-cataloguing-practices/), в котором рассказано об эволюции и текущем положении дел с практикой каталогизации электронных документов в Национальных Архивах. Также описаны наш подход и некоторые из проведенных к настоящему времени работ. В частности, в документе сказано о новом статусе и значении описания контекста для электронного архива:

«Практики каталогизации электронных документов в Национальных Архивах» (Digital Cataloguing Practices at The National Archives), март 2017, http://www.nationalarchives.gov.uk/documents/digital-cataloguing-practices-march-2017.pdf .

«Как изначально-электронные, так и оцифрованные документы сталкиваются с новой общей для них экзистенциальной проблемой: свойства документа, имеющие отношение к его достоверности, подотчетности, аутентичности и целостности – одним словом, к его «документности» – не присутствуют в самом электронном объекте, а отражены в сопровождающих

его метаданных, которые становятся неразрывно связаны с ним. В результате метаданные становятся частью документа».

Более подробно о нашей точке зрения на модели метаданных и их происхождение Вы можете узнать из недавно опубликованного поста «Семь столпов метаданных», см. http://blog.nationalarchives.gov.uk/blog/digital-archiving-seven-pillars-metadata/ – *перевод на русский язык доступен пол адресу* https://rusrim.blogspot.ru/2018/04/blog-post_19.html .

«Мы будем изучать новые возможности для контекстуального описания»

У нас есть замечательные возможности для переосмысления того, как мы устанавливаем интеллектуальный контроль с использованием современных технологий в условиях, когда расширяется приём на хранение намного более насыщенных документов, с встроенной прямо в их структуру информацией о том, как они создавались и использовались. Хорошим примером тому являются сообщения электронной почты: каждое сообщение включает в себя обширную информацию о взаимосвязях и цепочках, о датах взаимодействия, о получателях и т.д.

Нам нужно не упустить возможности для захвата как можно большего количества сведений о контексте (при этом по-прежнему сохраняя для всего набора данных контекстную информацию о его ответственном хранении, которая поступает от источника комплектования в определенный момент времени). И нам нужно больше думать о компьютерных моделях, которые мы создаем для поддержки проведения экспертизы ценности и отбора документов. Мы начинаем разрабатывать системы машинного обучения, которые помогут нам в процессе отбора. В свою очередь информация о том, как эти системы разрабатываются и создаются, станет теперь важным элементом контекста, раскрывающим, почему некоторые электронные активы были сохранены, а другие - нет. Интересно, сколько же сведений пользователи захотят получить о системе, которая использовалась для выявления и отбора тех самых документов, которые им предоставлены?

«Мы будем изучать вопрос о том, как наилучшим образом управлять неопределенностью в наших данных о документах»

К настоящему моменту мы начали прием на хранение того, что рассматриваем как «первое поколение» электронного контента – это изначально-электронные документы, электронные суррогаты и оцифрованные документы (фактически, это электронные версии бумажных документов). Однако сейчас мы сталкиваемся с наплывом «необъезженного» второго поколения изначально-электронного контента, который уже накапливается в государственных ведомствах – с электронным «Диким Западом», где мы больше уже не можем полагаться на традиционные опоры в виде надежной аутентичности или ясности вопроса о том, кто создал документ, о его временных рамках и согласованности формата. Вероятно, будет чрезвычайно сложно обуздать эти не подчиняющиеся законам данные в рамках структур традиционного онлайн-каталога.

Когда мы используем контекстуальную информацию, которая была сгенерирована компьютером, мы не можем гарантировать ее абсолютную достоверность или релевантность. Возможно проникновение в метаданные определенных «ложных новостей» (fake news). Например, Вы может знать «дату последнего изменения» для документа, но какова вероятность того, что именно тогда файл действительно был последний раз существенно изменён? Такого рода знания о чём-либо мы можем отразить, используя «вероятностное описание» (probabilistic description).

«Практики каталогизации электронных документов в Национальных Архивах» (Digital Cataloguing Practices at The National Archives), март 2017, http://www.nationalarchives.gov.uk/documents/digital-cataloguing-practices-march-2017.pdf

«Вероятностное описание признает прозрачным образом то, что данные несовершенны и что в них присутствует неопределенность. Мы рассматриваем введение в наши будущие метаданные для изначально-электронных и других документов показателей уверенности (confidence ratings)».

Нам также необходимо принять во внимание то, что люди могут пожелать изучать совокупности электронных документов, а не отдельные документы, и это повлияет на информацию, которая им будет нужна о документах. Хотя мы по-прежнему предлагаем нашим «читателям» точку зрения, сфокусированную на отдельных документах, мы также должны делать документы доступными для анализа с применением вычислительных методов, позволяя «пользователям данных» работать с большими массивами документов и ставить исследовательские вопросы очень разных типов.

«Электронные документы могут устанавливать контекст друг для друга»

Есть ряд действительно захватывающих новых возможностей для установления контекста. Широкое распространение электронных документов в государственном управлении было соизмеримо с развитием «всемирной паутины». В настоящее время правительство выкладывает в публичном доступе гораздо больше информации о своей деятельности. Мы захватываем эти материалы в нашем веб-архиве правительства Великобритании (http://www.nationalarchives.gov.uk/webarchive/); и сейчас мы приближаемся к очень интересному моменту, когда мы сможем начать контекстуализацию электронных документов на основе тех подробных сведений о себе, которыми государственные органы делились в Интернете в соответствующие периоды времени. И, конечно же, существуют другие веб-архивы, которые дают более широкий контекст того, что происходило в Интернете – и в мире – в это время.

Внезапно у нас появится возможность контекстуализировать каждый документ в рамках множества документов, содержащихся в глобальной развернутой информационной системе. Нам нужно будет спланировать, каким образом мы могли бы с этой целью установить связи с другими веб-архивами и учреждениями, занимающимися сохранением культурно-исторической памяти.

Использовать преимущества «интертвингулярности»

Как объясняет Википедия, термин «интервингулярность», придуманный американским ИТ-пионером, философом и социологом Тедом Нельсоном (Ted Nelson), выражает сложность взаимосвязей человеческого знания (см. http://ru.knowledgr.com/00203928/Intertwingularity*), и искусственность и неэффективность попыток как-то его структурировать в виде относительно простых последовательных или иерархических структур. Конечно, можно было бы придумать термин попроще, типа «неразделимости знания», но это было бы неинтересно*).

Традиционный архивный каталог является иерархическим по структуре: до сих пор иерархия и структура были ключевыми элементами при предоставлении архивного контекста.

В «перевязанном» гиперссылками мире богатство контекста – интеллектуального контроля – намного больше, чем мы традиционно способны были достичь. Мы вступаем в эпоху, когда архивы смогут использовать преимущества того, что философ и социолог Тед Нельсон назвал «интертвингулярностью» (intertwingularity, https://en.wikipedia.org/wiki/Intertwingularity).

Тед Нельсон (Ted Nelson) «Компьютерная библиотека: Ты можешь и должен понять компьютеры сейчас / Машины мечты: Новые свободы через экраны компьютеров – отчет меньшинства» (Computer Lib: You can and must understand computers now/Dream Machines: New freedoms through computer screens - a minority report), 1974 год.

«Всё глубоко переплетено и тесно взаимосвязано. В существенном смысле, «научных дисциплин» нет вообще; есть лишь единое знание, поскольку перекрестные связи между бесчисленными вопросами этого мира просто невозможно аккуратно отделить».

Различные виды информации могут контекстуализировать друг друга. Карта окружной железной дороги, 1898 г. Код по каталогу RAIL 1034/69

Знания и информация о наших активах, которые пользователи в состоянии собрать воедино, находятся на грани того, чтобы стать неизмеримо более объёмными и детальными.

Нам в Национальных Архива предстоит проделать большую работу, чтобы быть уверенными в своей готовности справиться с богатством и сложностью направляющегося в нашу сторону прилива информации, – а также в том, что мы сможем обеспечить уровень интеллектуального контроля, на который будут рассчитывать наши пользователи. Это захватывающий вызов, и к настоящему времени нам удалось добиться впечатляющего прогресса по ряду направлений.

Если Вы работаете в этой области, или у Вас есть интерес к какой-либо из тем, затронутых в этом посте, мы будем рады услышать Ваше мнение. Пожалуйста, оставьте комментарий на блоге или напишите нам по адресу discovery@nationalarchives.gov.uk .

ДОКУМЕНТЫ И ДАННЫЕ В ОБЛАКЕ: ПРОБЛЕМЫ ЭТИКИ И ДОВЕРИЯ

Автор: Коринн Роджерс, Университет Британской Колумбии, Канада

В своем сегодняшнем выступлении я кратко познакомлю Вас с проектом InterPARES, который с 1998 года занимается изучением вопросов, связанных с аутентичностью электронных документов. Затем мы обсудим ряд вопросов этики и доверия, касающихся документов и данных, которые создаются, используются и хранятся в различных облачных сервисах, и будут представлены несколько инструментов для оценки проблем управления документами в облаке. Эти инструменты являются продуктами наших последних исследований, выполненных в рамках проекта InterPARES Trust. В частности, я расскажу о двух контрольных листах (один предназначен для оценки условий контрактов с поставщиками облачных услуг, а второй – для налаживания в облаке отслеживания сроков хранения и выполнения установленных действий по их истечении); а также о базовом руководстве по управлению документами, касающимися вовлечения граждан в инициативы «открытого правительства».

Аббревиатура InterPARES расшифровывается как «Международные исследования по аутентичным документам постоянного хранения в электронных системах» (International Research on Permanent Authentic Records in Electronic Systems). Сокращение также можно прочитать и как латинское выражение «inter pares» – «среди равных», что намекает на равноправные отношения между участниками проекта. Соответственно, InterPARES Trust – это четвёртый этап «Доверие» проекта InterPARES.

Первый этап проекта InterPARES (InterPARES 1) был начат Университетом Британской Колумбии (Канада) в 1998 году и продолжался три года. Его целью была разработка **теории и методов**, необходимых для обеспечения того, чтобы электронные документы, созданные в **базах данных** и **офисных системах**, могли бы считаться «документами» с точки зрения архивной науки, и чтобы можно было доказать сохранение ими аутентичности с течением времени. Исследователи поняли, что как в архивной науке, так и в юриспруденции, документы, созданные и используемые в рамках обычной повседневной деловой деятельности, могут обладать презумпцией аутентичности. Однако в электронных системах эти документы подвержены риску как непреднамеренных, так и умышленных модификаций или порчи. Исследователи изучали электронные документы с точки зрения стороны-хранителя, обеспечивающей их долговременную сохранность, задавая вопрос о том, как архивы должны обрабатывать эти объекты, когда они попадают на архивное хранение. В ходе проекта на основе дипломатики и архивной теории были разработаны концепции необходимых и достаточных компонентов электронного документа, а также шаблоны для анализа электронных материалов, а также оценочные и базовые требования для проведения оценки и обеспечения сохранности аутентичных документов в течение длительного времени.

На втором этапе проекта InterPARES сфера исследований была расширена на огромное разнообразие документов, создаваемые **в динамических, чувственно-эмпирических (experiential) и интерактивных системах** в ходе творческой и научной деятельности, а также деятельности электронного правительства. На этом этапе исследователи рассматривали электронные документы с точки зрения их создателей, ставя вопрос о том, что требуется для создания **точных и надёжных** документов и для их последующего хранения и обеспечения сохранности **в аутентичной форме**, – как в долгосрочной, так и в краткосрочной перспективе, будь то для использования их первоначальным создателем или же обществом в целом, и несмотря на устаревание технологий и «хрупкость» носителей информации.

Результаты проектов InterPARES 1 и 2 оказали большое влияние, но ряд специалистов критиковал их как реалистичные только для крупных, богатых ресурсами организаций. Был задан вопрос: а как быть небольшим организациям, имеющим одного-единственного архивиста и ограниченные финансовые ресурсы, при слабой или вообще отсутствующей поддержке со стороны их руководства? Этот вопрос был воспринят как вызов в проекте InterPARES 3, целью которого было внедрение теории на практике. Результаты InterPARES 1 и 2 были внедрены в рамках десятков практических примеров (case studies), с участием партнеров проекта по всему миру.

Результаты проекта InterPARES нашли своё отражение в законодательстве Италии и Китая; в стандартах, включая американский стандарт DoD 5015.2 (*знаменитый документ, разработанный американским военным ведомством и ставший первым сертификационным стандартом для систем управления электронными документами*), MoReq2 (*возможно, лучшие*

функциональные требования к системам управления электронными документами, разработанные на деньги Евросоюза), OAIS (*стандарт открытой архивной информационной системы – по сути, библия электронного архивного дела, ставшая международным стандартом ISO 14721*), и уже совсем недавно – в канадском национальном стандарте CAN/CGSB 72.34 «Электронные документы как документальное доказательство» (Electronic Records as Documentary Evidence), опубликованном 1 марта 2017 года (*о нём см пост* Натальи Храмцовской http://rusrim.blogspot.ru/2017/05/cancgsb-7234-2017.html). Эти результаты также повлияли на широкий спектр политик и процедур различных организаций, а также на учебные программы университетского обучения и повышения квалификации.

Результаты первых трёх этапов проекта InterPARES актуальны для всех типов электронных документов в деловых системах, равно как и для интерактивных и динамических систем отдельных лиц и организаций. Они также верны и для документов, которые сейчас создаются, поддерживаются и хранятся в облаке, - но их недостаточно. В этой связи Канадский совет по исследованиям в области общественных и гуманитарных наук (Social Sciences and Humanities Research Council, SSHRC, http://www.sshrc-crsh.gc.ca/) поддержал 4-й этап проекта InterPARES, направленный на изучения документов в онлайн-средах – документов в социальных сетях, «открытого правительства», о вовлечении граждан, а также деловых документов, создаваемых, управляемых, анализируемых, делаемых доступными, хранимых и, возможно, даже длительно сохраняемых в облаке.

Один из поставленных нами ключевых вопросов был следующим: Какое влияние оказывают постоянно действующие сетевые коммуникационные технологии и сервисы облачных вычислений на управление документами, на ведение заслуживающих доверия документов и на поддержку доверительного отношения клиентов / граждан к документам?

Все мы, наверное, знакомы со стандартным определением облачных вычислений, предложенным американским Национальным институтом стандартов и технологий (National Institute of Standards and Technology, NIST): «Модель обеспечения удобного сетевого доступа по требованию к совместно используемому пулу конфигурируемых вычислительных ресурсов, которые могут быть быстро предоставлены и высвобождены с минимальными усилиями по управлению и с минимальным взаимодействием с поставщиками услуг».

Эти услуги могут оказываться на основе одной из моделей развертывания (или их комбинации), у каждой из которых имеются свои достоинства и затраты.

Инфраструктура публичного облака предоставляется широкой общественности через Интернет. Публичные облака, являющиеся по определению внешними по отношению к клиентам организациями, принадлежат и управляются третьими сторонами – поставщиками услуг, и использование услуг регламентируется детальными соглашениями о качестве обслуживания. В число вызывающих озабоченность вопросов входят безопасность и защита персональных данных в среде обслуживания группы

клиентов (multi-tenancy environment) и проблемы с несколькими юрисдикциями.

Эти проблемы часто решаются путем использования инфраструктуры частного облака, используемой в интересах одной организации: данные в частном облаке не используют общие ресурсы с данными, принадлежащими другим лицам или организациям. Частное облако может управляться организацией или третьей стороной; и может размещаться в ИТ-инфраструктуре организации или вне её.

Между этими двумя вариантами находятся коллективные (community clouds) и гибридные облака. Инфраструктура коллективного облака совместно используется двумя или более организациями, имеющими одинаковую точку зрения на вопросы защиты персональных данных, обеспечения безопасности и исполнения законодательно-нормативных требований. Она может управляться самими организациями или третьей стороной, и может размещаться на собственной или внешней ИТ-инфраструктуре.

Наиболее сложным является гибридное облако, состоящее из двух или более облаков (частных, коллективных или публичных), которые остаются самостоятельными сущностями, однако тесно связаны друг с другом посредством стандартизованной или проприетарной технологии, которая обеспечивает перемещаемость данных и приложений.

Это определение может быть упрощено и сведено к самой его сути: облако – это не чей-то чужой компьютер, а наполненный однотипным оборудованием центр обработки данных, в котором каждый процесс развертывания, обновления, поиска и управления автоматизирован (Branscombe, 2017). Это означает, что наши документы и данные, в отношении которых законодательство может требовать их нахождения на нашем ответственном хранении и под нашим контролем, на деле в большей или меньшей степени управляются третьими сторонами.

Но почему, действительно, необходимы эти исследования? Если, как я уже сказала ранее, результаты предыдущих проектов применимы к электронным документам вне зависимости от их технической среды, зачем нужен ещё один исследовательский проект? Ответ можно увидеть в тех заявлениях по поводу облака, которые делают представители отрасли; в той спешке, с которой многие организации стремятся внедрять новейшие технологии; и в темпах развития и изменения технологий. Облако широко используется, но это в значительной степени обусловлено давлением рынка, при этом на управление документами и архивы обращается мало внимания.

Это иллюстрирует подборка цитат из публикаций основных отраслевых аналитиков – компаний Гартнер (Gartner) и International Data Corporation (IDC):

- «Стратегии использования облачных вычислений как предпочтительного решения (cloud-first) – основа для сохранения своих позиций в быстро меняющемся мире»;
- «Внедрение Облака в корпоративной среде действительно стало господствующей тенденцией: 68% компаний используют сейчас публичное или частное облако ... на 61% больше, чем в прошлом году ...»;

- «Чем больше масштабы внедрения облачных вычислений, тем выше степень получаемой деловой отдачи»;
- «В среднем в расчёте на одно развернутое в облаке приложение обследованные организации получают 3 млн. долл. дополнительной выручки и 1 млн. долл. сокращения затрат ...» (Mahowald et al., 2016)

Эти высказывания говорят о скорости разработки и внедрения облаков, а также о том, что основное внимание уделяется сокращению затрат и оптимизации получения отдачи.

Хотя ИТ-персонал, высшее руководство и политики могут жаждать прыжка в облако, ссылаясь на эффективность и финансовые выгоды, однако есть проблемы, которые необходимо решать. Чаще всего обсуждаются проблемы, «вращающиеся» вокруг данных, что отражает мышление, ориентированное на данные. Речь идёт о вопросах обеспечения безопасности данных и защиты персональных данных, о том, как обеспечить соблюдение законодательно-нормативных требований в случае передачи данных в другие юрисдикции, какие имеются гарантии непрерывности предоставления услуг и что делать в случае утечек данных. Сообщит ли Вам поставщик облачных услуг о произошедшей утечке, насколько быстро, и какие меры будут приняты для смягчения последствий?

Когда мы думаем с точки зрения управления документами, мы видим связанные с облачными вычислениями проблемы в ином свете. Мы храним документы в качестве свидетельств деятельности и как память о действиях, для обеспечения подотчетности – для этого мы должны доверять им. На языке архивной науки, мы доверяем документам в той степени, в которой можем доказать их аутентичность, надежность и точность. С точки зрения права (по крайней мере, в странах английского права), вопрос доверия изучается в рамках правил допустимости документальных доказательств. Способность представить доказуемую последовательность ответственного хранения (chain of responsible custody) является ключевым фактором в обоих случаях.

Проблемы, связанные с управлением документами, несколько отличаются от проблем, связанных с данными – документы являются таковыми в основном благодаря их контексту и наличию связей с их создателями; с операциями, в которых они участвовали или которые документировали; с другими документами, созданными в рамках той же деятельности – это то, что в архивной науке называется «архивной взаимосвязью» (archival bond). Соответственно, документо-ориентированное мышление требует постановки иных вопросов:

- Можно ли защитить и сохранить контекст документов?
- Можно ли доказать происхождение?
- Можно ли отследить сроки хранения и выполнить надлежащие действия по их истечении?
- Можно ли обеспечить во времени доступность и пригодность к использованию? и
- Можно ли соблюсти права интеллектуальной собственности?

Эти вопросы отражают те этические проблемы, которые специалисты в области управления документами и архивного дела давно решают в отношении аналоговых документов, – а теперь им придётся иметь дело с облачными системами:

- Как защитить конфиденциальность и неприкосновенность частной жизни, одновременно обеспечивая доступ;
- Обеспечение безопасности;
- Предоставление доступа всем, признавая в то же время, что не у всех пользователей имеется надежный доступ к Интернету – «цифровое неравенство» (digital divide);
- Уважение прав интеллектуальной собственности и управление ими;
- Решение юрисдикционных проблем;
- Внимательное отношение к вопросам управления идентицирующей информацией, к деидентификации данных и их потенциальной нежелательной ре-идентификации;
- Понимание предполагаемых и непреднамеренных последствий анализа данных, включая предвзятость и профилирование.

Этичность нашего поведения в отношении документов и данных может оцениваться в рамках концепции ответственности и доверия, и для этой цели часто используются кодексы профессиональной этики. Национальные профессиональные ассоциации обновляют свои кодексы этики, чтобы отразить эти новые или усложнившиеся проблемы – например, Ассоциация канадских архивистов (Association of Canadian Archivists, ACA) только что опубликовала новый кодекс профессиональной этики (*о нём см. также пост* http://rusrim.blogspot.ru/2017/06/blog-post_20.html). Среди профессиональных ассоциаций существует общий консенсус в отношении основных желательных принципов:

- Поддерживать интеллектуальную свободу и сопротивляться цензуре;
- Защищать неприкосновенность частной жизни и конфиденциальность;
- Признавать и уважать права интеллектуальной собственности.

Поэтому ответственность лежит на нас, и для того, чтобы начать решать эти проблемы и выполнять свои этические обязательства, нам нужно определить, что мы подразумеваем под доверием. В проекте InterPARES Trust, для целей исследований, «доверие» было определено как уверенность одной стороны в другой, основанная на согласованности систем ценностей сторон в отношении определенных действий или выгоды, и включающая отношения добровольной уязвимости, зависимости и опоры (reliance), основанные на оценке риска. Доверие субъективно, оно может варьироваться в непрерывном диапазоне от полного доверия до скептицизма и недоверия.

Достоверность записей также зависит от надежности систем записей, в которых они создаются, управляются и хранятся. И поэтому это возвращает нас к облачным сервисам, которые соответствуют нашим стандартам как надежные системы записей?

Документы признаются заслуживающими доверия на основе презумпции их аутентичности и на основе оценки их надежности и точности. Доверие к документам также зависит от доверия к документным системам, в которых они создаются, поддерживаются и хранятся. И это возвращает нас к облаку - отвечают ли облачные сервисы стандарту доверенных документных систем?

Я собираюсь представить три инструмента, разработанных в ходе проекта InterPARES Trust, которые помогут принимающим решения лицам оценить преимущества и риски облачных услуг с точки зрения требований к управлению документами, основанных на архивной науке.

Инструменты, о которых я буду говорить сегодня, это

- Контрольный лист для оценки контрактов с поставщиками облачных услуг;
- Контрольный лист для оценки способности отслеживать в облаке сроки хранения и выполнять установленные действия по их истечении;
- Базовое руководство (primer) по управлению документами, касающимися вовлечения граждан в инициативы «открытого правительства».

Наиболее часто изучаемые в рамках InterPARES Trust отношения доверия – это отношения между потребителями облачных услуг (отдельными лицами или сообществами пользователей) и поставщиками облачных услуг (cloud service providers, CSP) в процессе потребления облачных услуг. Инструментами, посредством которых обеспечивается доверие, являются контракт на оказании услуг, соглашение об уровне/качестве обслуживания и/или условия предоставления услуг. Взаимоотношения между поставщиками облачных услуг и пользователями часто отражают неравенство сил: пользователь зависит от услуг поставщика, и у него мало шансов повлиять на условия их взаимодействия. Если государственные органы и крупные организации ещё имеют возможность договариваться об условиях своих контрактов с этими поставщиками, у большинства из нас нет иного выбора, кроме как принять типовые контракты, подготовленные поставщиками услуг. Положения типовых контрактов обычно формулируются доминирующей в контрактных взаимоотношениях стороной таким образом, чтобы соответствовать её целям, и не подлежат обсуждению.

Для того чтобы контракт был инструментом доверия, его условия должны быть прозрачными, понятными и всеобъемлющими с точки зрения наших потребностей. Для этого требуется, чтобы мы с самого начала сформулировали наши потребности и требования. К сожалению, беспокоящие специалистов по управлению документами вопросы - такие, как защита аутентичности документов, отслеживание сроков хранения и выполнение установленных действий по их истечении, наличие метаданных, подтверждающих происхождение документов и непрерывную последовательность ответственного хранения – редко всерьёз заботят лиц, принимающих решения об аутсорсинге ИТ-функций в облако.

ПЕРЕЛІК МІЖНАРОДНИХ СТАНДАРТІВ, ЯКІ ОПРАЦЬОВАНО ТА ПРОАНАЛІЗОВАНО НДІ МІКРОГРАФІЇ ЗА І ПІВРІЧЧЯ 2018 РОКУ

Автор: Шевченко І. І.

Науково-дослідний, проектно-конструкторський та технологічний інститут мікрографії (далі − НДІ мікрографії) проводить науково-дослідну роботу з дослідження та аналізу міжнародних стандартів ISO та розроблення рекомендацій щодо гармонізації нормативної бази державної системи СФД з міжнародною.

За І півріччя 2018 року проведено аналіз 19 міжнародних стандартів міжнародних технічних комітетів стандартизації:

– ISO/TC 42 «Фотографія»;

– ISO/TC 46 «Інформація та документація»;

– ISO/TC 171 «Управління документообігом»;

– ISO/TC 292 «Безпека», з якими НДІ мікрографії веде співробітництво та є їх членом.

Перелік міжнародних стандартів, які проаналізовано за поточний період:

1. ISO/DIS 18948 Зображувальні матеріали − Фотокниги − Методи випробувань для перевірки сталості та довговічності (Imaging materials – Photo books – Test methods for permanence and durability);
2. ISO/DTR 22428 Інформація та документація – Управління записами в «хмарі»: ризики та проблеми (Information and documentation – Records management in the cloud: Issues and concerns);
3. ISO/CD 30300 Інформація та документація – Управління документацією – Основні поняття та словник (Information and documentation – Records management – Core concepts and vocabulary);
4. ISO/DIS 24517-2 Управління документообігом – Технічна документація у форматі PDF – Частина 2: Використання ISO 32000-2, що включає довгострокове зберігання (PDF/E-2) (Document management – Engineering document format using PDF– Part 2: Use of ISO 32000-2 including support for long-term preservation (PDF/E-2);
5. ISO/CD 22550 Управління документообігом – Набір AFP для обміну і набір функцій для PDF (Document management – AFP Interchange Set and Function set for PDF);
6. ISO/DTR 22957 Управління документообігом – Аналіз, вибір та впровадження систем управління корпоративним контентом (ECM) (Document management – Analysis, selection and implementation of enterprise content management systems (ECM);
7. ISO/SR 8126 Мікрографія – Контратипні срібні діазо- та везикулярні плівки – Візуальна густина – Технічні вимоги та вимірювання (Micrographics –

Duplicating film, silver, diazo and vesicular – Visual density – Specifications and measurement);
8. ISO/DIS 22327 Безпека та стійкість – Управління надзвичайними ситуаціями – Настанови для впровадження на місцевості системи раннього попередження зсуву (Security and resilience – Emergency management – Guidelines for implementation of a community-based landslide early warning system);
9. ISO/SR 22300 Безпека та стійкість – Словник (Security and resilience – Vocabulary);
10. ISO/SR 21550 Фотографія – Електронні сканери для фотографічних зображень – Вимірювання динамічного діапазону (Photography – Electronic scanners for photographic images – Dynamic range measurements);
11. ISO/SR 6148:2001 Фотографія – Мікрографічні плівки, котушки та осердя – Розміри (Photography – Micrographic films, spools and cores – Dimensions);
12. ISO/DTR 21946 Інформація та документація – Оцінка управління записами (Information and documentation – Appraisal for managing records);
13. AS/NZS ISO 13028 Інформація і документація – Рекомендації щодо оцифрування документів (Information and documentation – Implementation guidelines for digitization of records);
14 ISO/DIS 21248 Інформація та документація – Оцінка якості національних бібліотек (Information and documentation – Quality assessment for national libraries);
15 ISO/FDIS 20247 Інформація та документація – Ідентифікатор міжнародної бібліотеки (ILII) (Information and documentation – International library item identifier (ILII));
16. ISO/SR 12656 Мікрографія – Використання штрихових кодів на апертурних картах (Micrographics – Use of bar codes on aperture cards);
17. ISO/SR 32000-1 Управління документами – Портативний формат документа – Частина 1: PDF 1.7 (Document management – Portable document format – Part 1: PDF 1.7);
18. ISO/SR 28004-1 Системи управління безпекою для ланцюга постачання – Керівні принципи для впровадження ISO 28000 – Частина 1: Загальні принципи (Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles);
19. ISO/SR 22315 Соціальна безпека – Масова евакуація – Методологічні рекомендації щодо планування (Societal security – Mass evacuation – Guidelines for planning).
Результати аналізу 8 міжнародних стандартів запропоновано фахівцям НДІ мікрографії щодо розгляду можливості застосування в наукових роботах, які виконують згідно з Тематичним планом прикладних досліджень та дослідно-конструкторських (технологічних) робіт НДІ мікрографії на 2018 рік та під час виконання робіт у перспективі.
Також матеріали чотирьох міжнародних стандартів за напрямом «Безпека» рекомендовано працівникам Українського науково-дослідного інституту цивільного захисту під час розроблення нормативних документів.

Дослідження та аналіз міжнародних стандартів надають можливість накопичувати світовий досвід з подальшим використанням його під час розроблювання нормативних документів комплексу СФД та у процесі впровадження провідних інформаційних технологій, технологічних процесів відповідно до вимог європейської системи технічного регулювання.

ЗМІСТ