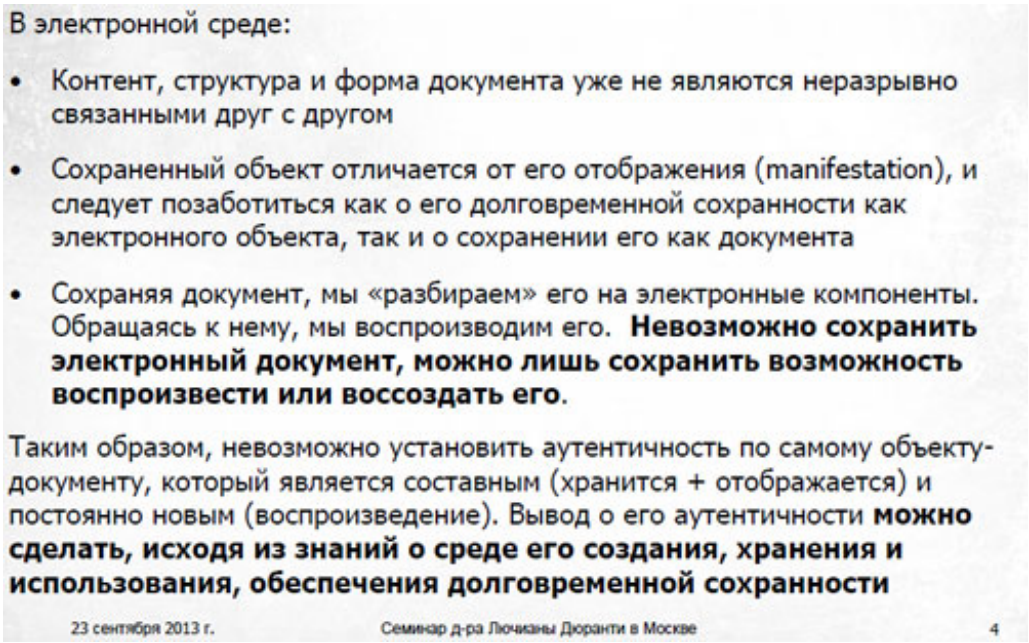
Семинар ЭОС и Лючиана Дюранти: новейшие тенденции в области управления электронными документами

spbit.ru /news/n97723/

Вчера, 23 сентября 2013 года, в Москве компания «Электронные офисные система» (ЭОС) провела семинар «Электронные документы: обеспечение аутентичности, долговременной сохранности и доверия» с участием одного из ведущих международных экспертов в этой области - руководителя кафедры архивно-библиотечного дела Университета Британской Колумбии (Канада), - Лючианы Дюранти. На встрече были затронуты такие темы как специфика электронных документов, проблемы, возникающие с хранением и передачей их через Интернет, вопросы аутентичности и целостности, а также аутентификации, обеспечения безопасности и пр. Кроме того, г-жа Дюранти рассказала о новом этапе своего международного проекта InterPARES Trust, призвав собравшихся к участию в нем. Стать другом проекта

Начиная свое выступление, г-жа Дюранти очертила круг проблем, связанных с самой природой электронных документов, а также, вытекающих из этого проблем обеспечения и поддержания во времени их доказуемой точности, надежности, аутентичности, а также, прозрачности и конфиденциальности одновременно. При этом, особое внимание должно уделяться развитию инфраструктуры, обеспечивающей плавный контролируемый поток аутентичных данных /контента/ документов от создателя к хранителю вне зависимости от изменений в технологии. Поэтому в целом, по ее словам, решения связанных с электронными документами проблем по своей природе являются динамичными и специфическими для каждой конкретной культурной, отраслевой, административной и правовой ситуации. А обеспечение долговременной сохранности представляет собой непрерывный процесс, который начинается с момента создания документа.

Говоря о специфике природы электронного документа, Лючиана Дюранти отметила, прежде всего, что контент, структура и форма такого документа не являются неразрывно связанными друг с другом. Сохраняя электронный документ, его «разбирают» на электронные компоненты, а при чтении, - снова собирают. Таким образом, по словам г-жи Дюранти, невозможно установить аутентичность по самому объекту- документу, который является составным (хранится + отображается) и постоянно новым (воспроизведение). Вывод о его аутентичности можно сделать только, исходя из знаний о среде его создания, хранения и использования, обеспечения долговременной сохранности. Соответственно, в условиях того, что практически все сегодня пользуются Интернетом для хранения и передачи своих данных, обеспечение аутентичности, конфиденциальности и безопасности электронных документов, особенно с учетом их специфики, представляет собой нетривиальную задачу.



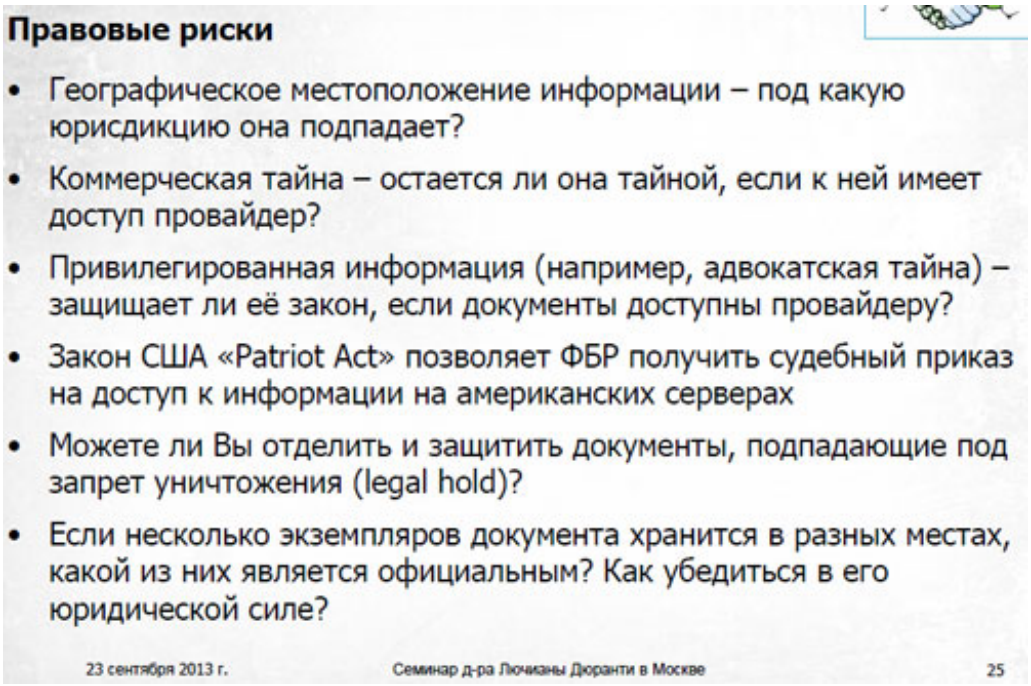
Электронные документы в сравнении с традиционными

«Фактически мы очень мало знаем о том, что происходит в Интернете. Доверие к Интернету строится на том же принципе, что и доверие на обычном рынке – caveat emptor (качество на риск покупателя), - когда покупатель должен сам проявлять надлежащую осмотрительность. В результате, - отношения доверия в Интернете в силу своей природы чреваты рисками, когда авторство, право собственности и юрисдикция могут быть поставлены под сомнение. Соответственно, при принятии решения об использовании Интернет-услуг необходимо оценить возможные риски, а также осознать то, чем в итоге придется пожертвовать ради получаемой отдачи. Поэтому здесь всегда существует два выбора: между прозрачностью и защищённостью; между контролем и экономической эффективностью» - рассказывает руководитель кафедры архивно-библиотечного дела Университета Британской Колумбии (Канада) Лючиана Дюранти.

Доктор Лючиана Дюранти, фото с сайта unidoc.coinfo.net

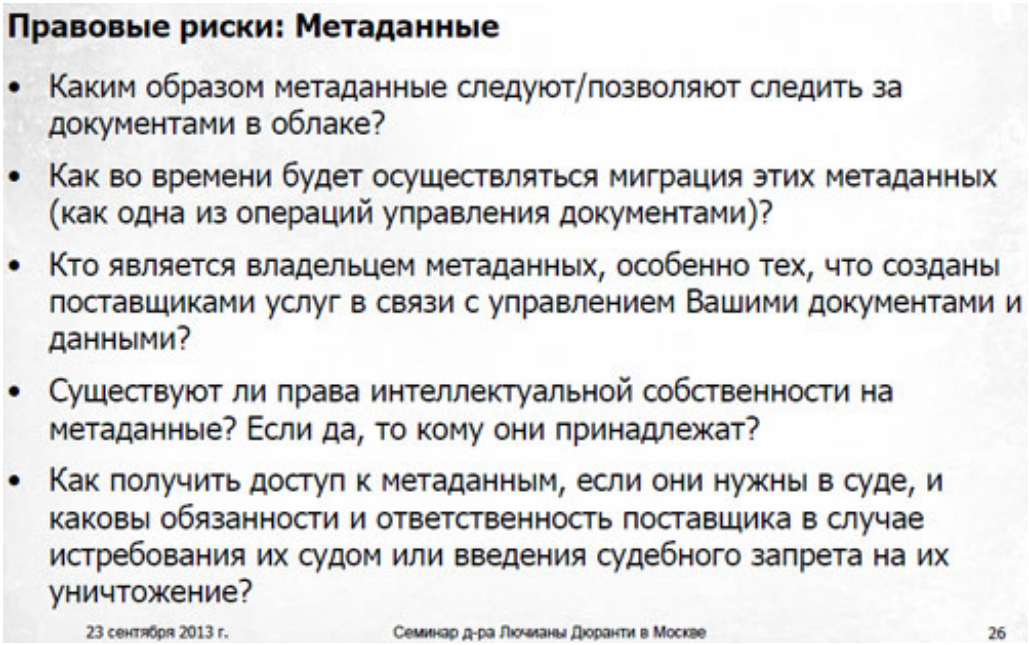
Помимо очевидных рисков, связанных с обеспечением безопасности данных в Интернете (несанкционированный доступ, передача информации субподрядчикам, хакерские атаки), необходимо также учитывать риски, связанные с отсутствием реального контроля над документами в онлайн-среде (вы не знаете, кто использует те же сервера и кому делегируется оказание услуг, не можете контролировать процесс копирования и уничтожения, а также полной передачи информации при переходе к другому провайдеру). Кроме того, следует учитывать и риски, связанные с невозможностью обеспечения полной прозрачности всех онлайн-операций с документами, когда трудно подтвердить непрерывную преемственность ответственного хранения (chain of custody), а на основе знаний об известных процессах невозможно сделать вывод о надёжности документов и их аутентичности, потому что известны доказанные случаи махинаций с документами в Интернете.

При этом, документы в Интернете не обладают целостностью с точки зрения судебной экспертизы (forensic integrity), для которой требуются такие качества, как повторяемость, проверяемость, объективность. Поэтому остается под вопросом, могут ли такие документы приниматься судом в качестве надлежащих доказательств.



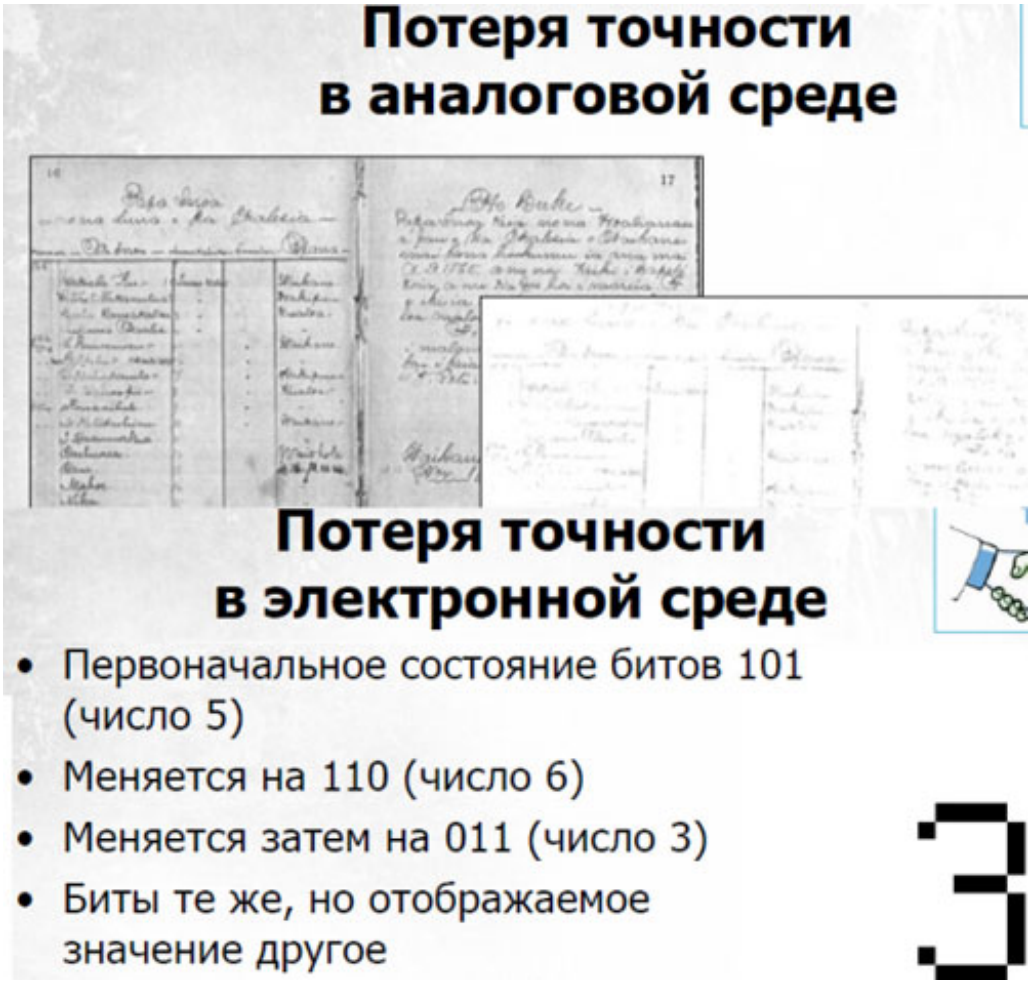
Правовые риски, связанные с размещением, хранением и передачей документов через Интернет

«Если мы хотим вести деловую деятельность в онлайн- среде, то следует найти баланс между доверием к партнеру и его надёжностью (trustworthiness), необходимый для сбалансированных отношений доверия. Доверие представляет собой риск, который можно снизить лишь благодаря балансу доверия (trust balance): мы должны доверять лишь тем партнерам и документам, которые заслуживают доверия. При этом, взаимоотношение доверия между доверителями и доверенными лицами обычно опирается на четыре характеристики доверенных лиц: репутацию, эффективность деятельности; уверенность; компетентность. При этом, в электронной среде вывод об аутентичности делается на основе базовых доказательств (foundation evidence – достаточные предварительные доказательства аутентичности и относимости представляемых материалов для допустимости их в качестве доказательств), и, в какой-то мере, - уверенности в эффективности и компетентности хранителя материалов, основанной на его репутации. Для того же, чтобы гарантировать аутентичность электронных документов, требуются сознательные действия или вмешательство доверенных лиц, подкреплённые как их подотчетностью, так и адекватным набором политик, процедур и технологий. Так было всегда» - продолжает г-жа Дюранти.



Правовые риски при онлайн-хранении документов, связанные с метаданными

В то же время, по словам Лючианы Дюранти, заслуживающий доверия документ, как правило, - все время больше, чем просто аутентичный, - он должен обладать также надежностью, точностью, целостностью. Под надежностью следует понимать доверие к документу как к констатации факта, основанное на компетентности его автора, его полноте и на мерах контроля над процессом его создания (ключевую роль играет источник документа). Точность в этом контексте означает доверие к правильности и детальности контента документа, основанное на перечисленных выше факторах, а также на мерах контроля над процессами фиксации и передачи контента (точность электронных объектов обеспечивается в том случае, если они повторяемы, repeatable). И, наконец, аутентичность, - это доверие к тому, что документ является именно тем, чем представляется, что он не был искажён или скомпрометирован, основанное на его идентифицирующих признаках и целостности, а также на надежности документной системы, в которой он находится. При этом, аутентичность опирается на контекст (процедурная, документальная и технологическая среды, в которой документ был создан и использовался с течением времени), идентификацию (совокупность атрибутов документа, которая характеризует его как уникальный объект и отличает от других документов) и целостность (документ является целостным, если сообщение, которое он должен передавать для достижения своей цели, не изменяется).

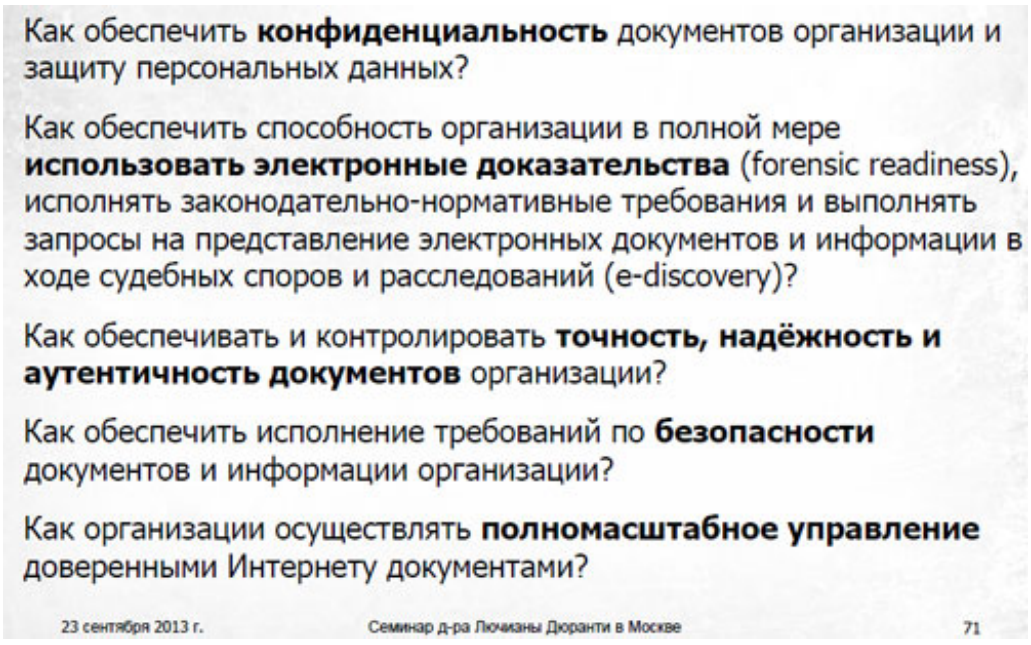


Разница с обеспечением целостности бумажных и электронных документов

При этом, целостность данных обеспечивается на основе концепции побитовой целостности: том факте, что данные не подвергались несанкционированной модификации, как умышленной, так и неумышленной. То есть исходные биты сохраняются в полном и неизменном состоянии с момента захвата, сохраняя один и тот же порядок и значение. Так как даже небольшие изменения в битах могут привести к отображению совсем иного значения на экране или к выполнению иных действий в программе или в базе данных. И если преднамеренные изменения можно предотвратить путем управления правами и использования мер и средств контроля доступа, то для защиты от случайного изменения требуется установка дополнительного оборудования и/или программного обеспечения (нужен метод, позволяющий установить, был ли документ злонамеренно либо неумышленно изменён). При этом, нельзя полагаться на размер файла, даты и иные свойства файла, - необходимы журналы аудита (логи), а также такие сильные методы, как алгоритмы подсчета контрольных сумм и вычисления хешей.

Предпочтительные средства аутентификации (вместо ЭЦП)

Что же касается обеспечения аутентичности электронного документа, то такие средства должны проводить аутентификацию в один конкретный момент времени, и, возможно, без учёта других доказательств идентичности (identity) и целостности. В качестве примера г-жа Дюранти привела электронную цифровую подпись (digital signature), которая функционально эквивалентна печати, а не подписи. ЭЦП позволяет: проверить происхождение документа (идентичность); удостоверяет его неизменность (целостность); обеспечивает неотказуемость. В то же время, есть и специфика, - если печати на бумажном носителе ассоциированы с лицом, то ЭЦП ассоциированы с лицом и с документом. В то же время, Лючиана Дюранти отметила, что ЭЦП не являются предпочтительным средством аутентификации во времени, так как их использование предпочтительно лишь в пространстве (ЭЦП очень быстро морально устаревают, кроме того, - невозможно обеспечить их долговременную сохранность). Из прочих факторов, мешающих широкому использованию ЭЦП г-жа Дюранти также выделила ее технологическую сложность, а также ограниченную зону использования в рамках концепции «разумной достаточности». Так, ЭЦП незаменима для защищенной передачи конфиденциальных сведений, персональных данных, ответственных финансовых транзакций и другой подобной информации, - но в остальных случаях ее использование является чрезмерным. Это приводит к тому, что при использовании ЭЦП в работе с обычными документами риск причинения ущерба выше, чем те риски, от которых электронная цифровая подпись должна защищать.



Вопросы для изучения в рамках проекта InterPARES Trust

Во второй части презентации Лючиана Дюранти рассказала о новом этапе своего международного проекта InterPARES (International Research on Permanent Authentic Records in Electronic Systems – «Международные исследования по аутентичным документам постоянного хранения в электронных системах»). Этот этап (InterPARES Trust) имеет целью создание теоретических и методологических основ, которые будут реализованы в конкретных политиках и нормативных документах, призванных обеспечить общественное доверие к электронным документам в Интернете. В заключение своего выступления г-жа Дюранти призвала собравшихся к участию в проекте, полную информацию по нему можно найти на официальном сайте www.interpares.org.

Напомним, что доктор Лючиана Дюранти является одним из наиболее уважаемых и известных в мире специалистов в вопросах, связанных с «жизненным циклом» электронных документов. С ее именем связан ряд крупнейших проектов, благодаря которым электронные документы стали реальностью современной жизни. Компания «Электронные Офисные Системы» (ЭОС) давно сотрудничает с Лючианой Дюранти в совместных проектах. В частности, эксперты ЭОС участвовали в создании общеевропейского стандарта MoReg2 и базы данных архивной терминологии Международного Совета архивов.