ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду архівних установ світу щодо вирішення проблем управління інформацією та документацією, а також довгострокового зберігання електронних інформаційних ресурсів.

У публікації «Проблемы управления информацией и документацией» розповідається про взаємодію IT-спеціалістів та фахівців з управління документацією в вирішенні виробничих завдань.

У публікації «Современные вирусы касаются каждого пользователя и напрямую нацелены на финансы» наведено відповіді на питання і корисні поради як захистити себе від вірусописьменників і хакерів.

У публікації «О мошенничестве с электронными подписями» описано способи шахрайських дій з електронними підписами на документах.

У публікації «Положение о Российском страховом фонде документов библиотек (РСФДБ)» наведено зміст Положення про Російський страховий фонд документів бібліотек.

У публікації «Евросоюз определился с форматами электронных подписей и печатей, используемых при получении государственных электронных услуг» розповідається про введення в дію рішення Єврокомісії 2015/1506 від 8 вересня 2015 року, яким встановлено вимоги до форматів посилених електронних підписів і посилених печаток.

У публікації «Ричард Пирс-Мозес: Что нужно знать архивистам?» наведено думку автора на професійні та технічні знання та навички, потрібні архівістам для виконання основних видів своєї діяльності в майбутньому.

У публікації «Австралия: Положение дел с хранением физических документов в государственных органах штата Виктория» розповідається про аналіз оцифровки документів організацій який проведено Управлінням державних документів австралійського штату Вікторія. Після проведення оцифровки окремі організації зберігають як вихідні паперові документи, так і їх електронні копії, що збільшує тягар адміністративних витрат.

У публікації «Франция: Подтекание трубопроводов в хранилище Национальных Архивов в Фонтенбло» розповідається, що підтікання трубопроводів в сховище філії Національних Архівів Франції в Фонтенбло призвело до замокання 33000 документів.

ПРОБЛЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И ДОКУМЕНТАЦИЕЙ

Источник: http://www.eos.ru/eos_delopr/eos_lib/detail.php?ID=131465&SECTION_ID=676

Информационные технологии сейчас активно используются в органах государственной власти и в коммерческих организациях, в том числе и для решения задач управления информацией и документацией. В данной области интересы ИТ-специалистов и специалистов по управлению документацией пересекаются, и им необходимо действовать совместно, но этому нередко мешает неумение понять точку зрения друг друга.

Поговорим о проблемах именно с точки зрения специалистов по управлению документацией, которых больше волнуют не технологические детали организации работы, а вопросы права и соблюдение установленных законодательно-нормативных требований. В конечном счете отличие документов от информации заключается в том, что документы имеют юридическое значение, с их помощью подтверждаются права и обязанности лиц и организаций, фиксируются результаты деловых операций и управленческие решения.

К сожалению, наши коллеги из ИТ не всегда осознают, что все сколько-нибудь существенные деловые решения и решения в области государственного управления принимаются на основе именно документированной информации (документов), а не информации «вообще».

Решить основные проблемы в области управления электронными документами и информацией, где тесно переплетены организационные и кадровые вопросы, вопросы технологий и права, можно только при слаженной работе междисциплинарной команды. Профессионалы в области управления документацией совместно с юристами, ИТ- и ИБ-специалистами и другими заинтересованными сторонами должны наладить такую систему управления информацией и документами, которая позволяла бы эффективно вести деятельность, обеспечивала прозрачность и подконтрольность государственного управления, а также надежно защищала собственные интересы организаций. Представители нашей профессии не собираются «закапываться» в бумажные документы, и опыт показывает, что взаимодействие с другими специалистами очень полезно для всех сторон, и что вместе мы можем сделать гораздо больше и лучше, чем по одиночке.

Этапы электронной революции

Электронная революция в управлении документами и информацией продолжается уже в течение довольно длительного времени, и в ее развитии можно выделить два этапа. Отмечу, что на практике оба они сосуществуют одновременно, что создает дополнительные проблемы.

Первый этап

Он связан, прежде всего, с переводом бумажных документов в «бумагоподобные» электронные документы. Параллельно начинают создаваться и все шире использоваться государственные базы данных, реестры и регистры. Еще быстрее меняют технологии своей работы коммерческие организации, внедряющие многочисленные информационные ресурсы, накапливающие и перерабатывающие документы и информацию.

Постепенно именно базы данных, а не бумагоподные электронные документы превращаются в основной инструмент принятия юридически значимых решений как в государственном управлении, так и в практической деятельности. Одновременно для большей оперативности и эффективности принятия решений автоматизируются бизнес-процессы и процедуры, что позволяет ряд юридически значимых, но рутинных действий выполнять в автоматическом режиме.

Использование информационных систем привело к тому, что при взаимодействии с государственными органами и коммерческими организациями их контрагентам уже не нужно повторно представлять документы, если они либо содержащиеся в них сведения имеются в государственных органах. Такая информация запрашивается у ее обладателя, получается и используется в электронном виде (сейчас это, как правило, бумагоподобные электронные документы, подписанные тем или иным видом электронной подписи).

Второй этап

Он характеризуется тем, что традиционный обмен документов постепенно уступает место коллективной работе с использованием государственных реестров и регистров. Значительная часть деловых решений принимается автоматически. Становится все меньше документов «прямого действия» (то есть таких, которые сами по себе вызывают желаемые последствия), а документы личного хранения, в том числе и те, что удостоверяют основополагающие права граждан и организаций, нередко превращаются в «ссылки» на информацию в соответствующих базах данных. Все чаще правовое значение имеют лишь документированные сведения, содержащие в информационных системах государственных органов и организаций.

Следует иметь в виду, что внедрение современных технологий идет неравномерно. Если судить по наиболее передовым организациям (налоговая и таможенная службы, банки и т. п.), мы уже переходим ко второму этапу электронной революции. Причем существует «многоукладность» технологий: даже в рамках одной организации можно встретить подразделения, использующие только бумажные или электронные технологии, а также существуют самые разнообразные промежуточные варианты.

Как и во всех революционных преобразованиях, в ходе этих перемен возникает ряд серьезных проблем, непосредственно связанных с управлением документами.

Проблема, связанная с законодательно-нормативной и методической базой

При работе с документами необходимо опираться на законы и подзаконную нормативно-правовую базу. До 2009 года использование электронных документов в государственном управлении и деловой деятельности законодательством регулировалось лишь рамочно. Применение новых технологий в основном происходило в рамках договорных обязательств на основе Гражданского кодекса. Примерно с 2009 года начался процесс бурного внедрения электронных документов во все сферы деятельности, и они стали все чаще приниматься судами в качестве доказательств. С 2010-го арбитражные суды сами перешли на электронное судопроизводство, понемногу этот процесс развивается и в сфере гражданского судопроизводства. ДЕЛО уже дошло до появления электронного нотариата.

Информационные технологии очень быстро меняются, обновляясь каждые 5–7 лет, и, как следствие, возникает необходимость в постоянном оперативном совершенствования и актуализации законодательства. В результате складывается сложная правовая ситуация: имеющееся на данный момент российское законодательно содержит массу противоречий и недостатков в области управления документами, и при этом постоянно меняется. В вопросах применения электронных документов законодатель часто перестраховывается, что особенно сильно проявляется при использовании электронных подписей.

По сути, сейчас в самых различных областях деятельности решается задача признания электронных документов полноправными и как минимум равноценными бумажным и, соответственно, придания им юридической и доказательной силы.

Но, несмотря на то что у существующей законодательно-нормативной базы есть проблемы, она уже сейчас позволяет использовать все большее число видов документов в электронном виде. Объемы создаваемых электронных документов все время растут, а вот норм, которые бы регулировали процедуры обеспечения их надежного хранения, пока не выработано.

Проблема долговременного хранения электронных документов

Наиболее сложной, с моей точки зрения, и до сих пор нигде в мире в полном объеме не решенной является проблема обеспечения сохранности электронных документов без ущерба для их юридической значимости и доказательной силы, особенно в случае, когда они подписаны усиленными электронными подписями (УЭП) или ЭЦП. Проблема здесь не в том, чтобы

сохранить содержащуюся в документах информацию – подобный опыт существует начиная с 1960-х годов, а в том, чтобы сохранять электронные документы таким образом, чтобы спустя 10, 50, 100 и более лет их нельзя было бы оспорить и поставить под сомнение. Учитывая, как быстро устаревают информационные технологии, как легко манипулировать электронными объектами и как быстро взламываются системы защиты, это очень непростой вопрос.

В мире, например, для обеспечения долговременной сохранности электронных документов уже предложен и опробован ряд решений, которые наши специалисты оценивают как вполне приемлемые, однако приходится учитывать, что ни одно из этих решений пока не опирается на действующее российское законодательство. К сожалению, мало придумать логичную и надежную технологию, нужно еще и убедить законодателя одобрить ее.

Именно поэтому эксперты в области управления документами говорят о том, что сейчас без особого правового риска подписывать усиленными электронными подписями можно документы со сроками хранения 5–7 лет. А вот создавать документы длительного срока хранения исключительно в электронном виде, с моей точки зрения, пока что рискованно, хотя в ряде случаев иного выбора просто нет. Отмечу, что в российском законодательстве уже есть ряд норм, требующих создавать и хранить в электронном виде документы длительного и постоянного сроков хранения.

Проблема создания нормально функционирующей и заслуживающей доверия PKI-инфраструктуры отрытых ключей

Широкомасштабное использование УЭП (а в данном вопросе Россия является мировым лидером) требует особого внимания к созданию обеспечивающей доверие к подписям инфраструктуры открытых ключей (PKI). Применяемая в настоящее время формальная процедура аккредитации в Минкомсвязи удостоверяющих центров, имеющих право выпускать универсально применяемые усиленные квалифицированные подписи, с самого начала вызывала серьезные претензии. Уже появилось более 300 таких центров (в любой другой стране их обычно 1–4), но доверия к большинству из них немного, хотя закон обязывает верить им одинаково! В настоящее время в Государственную Думу внесен законопроект, направленный на ужесточение требований к УЦ.

Очень мало внимания уделяется вопросам документирования деятельности удостоверяющих центров, связанной с выпуском и отзывом сертификатов ключей подписи. Следует помнить, что если усиленной подписью подписан документ длительного или постоянно срока хранения, то для того, чтобы впоследствии иметь возможность заново проверить подпись, вместе с этим документом необходимо хранить не только сертификат ключа проверки, но и доказательство того, что этот сертификат не был отозван ранее времени подписания электронного документа. Сама процедура проверки «исторических» УЭП/ЭЦП также требует регламентации. Если эти

вопросы не решить, то уже в ближайшее время и система государственного управления, и бизнес могут столкнуться с проблемой подтверждения юридической значимости электронных документов, созданных лишь несколько лет тому назад.

Появление новых видов электронных документов и документированной информации

В настоящее время в государственном управлении и в бизнесе используются и такие виды электронных документов, которые плохо вписываются в традиционную российскую систему делопроизводства. Как следствие, изменяется вся система и процессы обработки документов, причем значительная часть документов начинает поступать к исполнителям напрямую, минуя «узкое горлышко» единой точки регистрации и контроля исполнения. В итоге сложно обеспечить захват этой деловой переписки в документные системы организаций. Мобильные и облачные вычисления еще больше все усложняют. В результате организации отчасти теряют контроль над своими документами, особенно над деловой перепиской, ведущейся по электронной почте, с использованием социальных сетей и т. п.

Технические решения подобной проблемы существуют, но большинство из них чрезвычайно обременительно для рядовых исполнителей, дороги для предприятий и трудоемки в реализации.

Проблемы защиты персональных данных

Активное использование электронных документов остро поставило и вопрос о необходимости надежного обеспечения защиты персональных данных. В современных условиях необходимо найти тонкий баланс: с одной стороны, обеспечить защиту интересов граждан и их персональной информации, а с другой – не довести дело до абсурда, когда необоснованные меры защиты мешают жить и работать, а также приводят к утрате исторической памяти. Например, последние решения Евросоюза по данному вопросу приводят к тому, что по требованию отдельных лиц из публичного доступа фактически изымается каким-то боком связанная с этими лицами информация, не содержащая ничего противозаконного (например, неблагоприятная рецензия на театральный спектакль).

Открытое правительство и открытые данные

Реализация проектов «открытого правительства» и раскрытия информации в формате открытых данных также требует изменений в системе управления документами, поскольку ставится задача оперативно раскрывать значительные объемы информации, с учетом необходимости защиты секретной, конфиденциальной информации и персональных данных.

Прозрачность государственного управления и возможность повторного использования государственной информации – важные элементы современной системы управления. В то же время здесь до сих пор часто

применяются классические приемы и методы работы с документами, сохранившиеся еще с петровских времен, – очень трудоемкие и недостаточно эффективные.

Проблемы многоукладности и смешанного документооборота

Серьезной проблемой для успешного перехода в электронное «светлое будущее» является ныне существующая многоукладность российского делопроизводства и переход в деловой деятельности и государственном управлении не к электронному (как многие наивно считают), а к смешанному бумажно-электронному документообороту.

Как следствие, при принятии решений о выборе технологий приходится порой ориентироваться не на самые передовые методы работы, а на те, которые на текущий момент приемлемы для большинства контрагентов. Невозможность отказаться от использования устаревших технологий и каналов взаимодействия нередко не позволяет получить полновесную отдачу от внедрения систем электронного документооборота или систем управления контентом.

Подводим итоги

Перечисленные выше вопросы – это далеко не полный список проблем, которые в ближайшее время придется решать на всех уровнях управления во всех сферах деятельности. Отмечу, что реализовать такие задачи под силу только дружной и сплоченной команде специалистов разных профессий. В такую команду ИТ-специалисты могут принести свои знания об особенностях технологий, а специалисты по управлению документами – о том, как вписать технологии в существующие правовые рамки, обеспечивая надежную информационную и документационную деятельность организации.

СОВРЕМЕННЫЕ ВИРУСЫ КАСАЮТСЯ КАЖДОГО ПОЛЬЗОВАТЕЛЯ И НАПРЯМУЮ НАЦЕЛЕНЫ НА ФИНАНСЫ

Источник: http://delo-press.ru/articles.php?n=19304

Руководитель стратегических и GR проектов ЗАО «Лаборатория Касперского» Андрей Юрьевич Ярных отвечает на интересные вопросы Романа Аваляна и дает полезные советы. Каковы потери бизнеса от кибер-атак? Во что целятся злоумышленники, когда охотятся на частных лиц? Каковы правила безопасности в соцсетях? Какие пароли не надо себе выбирать? Как еще защитить себя и деньги от вирусописателей и хакеров?

– Андрей Юрьевич, тема нашего интервью – безопасность в интернете. Скажите, пожалуйста, насколько вообще опасен интернет?

– Приведу конкретные цифры. В 1994 году появлялся один новый вирус каждый час. Вирусный фон был тогда достаточно щадящий. Но и интернет был маленький. В 1996 году уже один новый вирус – каждую минуту. В 2011 году – один новый вирус каждую секунду. На сегодня мы детектируем 325000 образцов нового вредоносного программного обеспечения каждый день.

Причем если мы сравниваем эпохи развития, то интернет был сначала небольшим, затем он начал бурно расти и развиваться. В начале 90-х годов создание вирусов было, по сути, попыткой самоутвердиться и заявить о себе. В «нулевые» наступила эра ботнета, и тогда же появились элементы монетизации, желание заработать при помощи вирусов.

Ну а с 2010 наступила эпоха целевых атак, когда нападают на компьютеры банков, других значимых структур, отдельных пользователей. Конечно, вирусы прошлого нельзя назвать совсем уж безобидными, потому что в те времена были вирусы, которые сжигали микросхемы. И тем не менее они зачастую были направлены на хулиганство. Например, затирали нулями первые 17 секторов жесткого диска. *Современные вирусы распространяются через эксплойты и спам*. Они несут значительно больший ущерб, касаются практически каждого пользователя и напрямую нацелены на финансы. *Проще говоря, злоумышленники крадут деньги.*

– Можно ли оценить потери бизнеса от кибератак?

– По нашим данным, потери крупного бизнеса от одной кибератаки в России оцениваются в 20 млн руб., малого и среднего – в 780 тыс. руб. Причем это средние заявленные потери. Понятно, что бизнес, особенно крупные коммерческие структуры, не горит желанием сообщать о своих инцидентах, так как это всегда удар по репутации. Поэтому цифры усредненные и на основе того, что известно. Мы предполагаем, что на самом деле ущерб больше, и в зоне риска находятся многие компании.

В пошлом году стали чаще атаковать банки. Причем использовались индивидуальные схемы, успешно заметались следы, и только благодаря успешной розыскной работе удавалось найти злоумышленников – разработчиков вредоносного программного обеспечения. Дело касалось не только зарубежных, но и российских банков. А одним из вирусов были заражены больше 1000 банкоматов по всему миру, в т.ч. в России, Европе, Азии, Северной Америке. А это влечет утечку, в том числе и вашей информации, которую вы, вставляя карточку в банкомат, можете потерять. Разумеется, в зоне риска и банки, у которых могут быть украдены деньги. Были случаи, когда целями являлись не конечные пользователи, а целый банк.

– Что крадут киберпреступники помимо денег? Интересует ли их какая-либо информация, хранящаяся на компьютерах компаний?

– Каждая третья компания теряла конфиденциальные данные. Важно отметить, что это очень серьезный репутационный риск. Наши опросы

показывают, что если информация о потере данных станет известной, то 91% опрошенных, узнав об этом, прекратят работать с компанией.

– Кто, наряду с банками, находится под угрозой?

– Все больше в зоне риска мобильные пользователи. На них совершается большое количество уникальных атак. Здесь прослеживается тот же самый вектор на охоту за деньгами.

По статистике в 53% финансовых атак используются мобильные банковские троянцы. Они открывают доступ к вашему устройству, скажем, к компьютеру или к планшету, после чего злоумышленник может закачать туда все что угодно, на свое усмотрение. Поэтому дальше возможны любые варианты использования компьютера или мобильного устройства. Из позитивного можно сказать, что СМС-троянцев за последний год стало на 12% меньше.

Если говорить о почтовых сервисах, то думаю, все помнят, как в прошлом году с трех популярных общедоступных почтовых сервисов «утекло» более 10 млн паролей. Поэтому пользователи почтовых сервисов тоже под угрозой.

– От пользователей MAC-устройств не раз доводилось слышать следующие слова: «А зачем нам защита? Мы защищены тем, что у нас уникальная операционная система». Действительно ли MAC-устройства настолько защищены?

– На самом деле уже есть пример ботнет сети под MAC-устройства.

Многие пользователи MACов и в частности iPhone уже столкнулись с неприятностью, когда их аккаунты блокировали. В Apple_ID есть возможность удаленного блокирования собственного устройства, если оно украдено. У многих такая опция была включена, и когда злоумышленники с помощью троянских программ или шпионского программного обеспечения получали доступ к логину Apple_ID, они использовали эти возможности для того, чтобы удаленно блокировать устройство пользователя. А потом просили деньги за разблокировку.

То есть фактически утечка такой информации, как логин и пароль к Apple_ID, привела к тому, что нормальные штатные механизмы, которые заложены в устройстве, злоумышленники используют для шантажа и вымогательства.

– Какие угрозы подстерегают пользователей в социальных сетях?

– В интернете все то, что вы выпустили из своих рук, сами о себе написали, вам уже не принадлежит. Вы даже удалить это нормально не сможете, потому что в кэше поисковых систем информация сохраняется. Поэтому с социальными сетями, да и вообще с любой информацией, размещаемой через интернет, надо быть очень аккуратными. Неосторожно размещенное фото в, казалось бы, защищенном режиме в какой-то момент может оказаться публичными. И это несет существенный репутационный риск и для медийных персон, и для обычных людей.

Все то, что пользователь размещает сам о себе, имеет высокую степень достоверности и откровенности. Но он в тот момент не предполагает, что размещенная информация может куда-то уйти и использоваться сторонними людьми, например, киберзлоумышленниками.

Пожалуй, главная угроза – это *кража пароля*. Например, киберпреступник может украсть логин и пароль при помощи вредоносного программного обеспечения. Или же при помощи уязвимости на стороне сервиса социальной сети злоумышленник может похитить учетные данные любого из ее клиентов и воспользоваться ими на свое усмотрение. И, пожалуй, наиболее тривиальный сценарий: злоумышленник может подобрать пароль к той или иной учетной записи так называемым методом «грубой силы» (bruteforce). Способы монетизации зависят от фантазии злоумышленника и количества взломанных аккаунтов. Так, например, обладая большим количеством скомпрометированных аккаунтов, злоумышленник может за определенную плату накручивать «лайки», выводить те или иные новости в «топ самых читаемых» и т.п. Или же, получив логин и пароль жертвы в социальной сети, мошенник может ее шантажировать угрозой полного удаления учетной записи или публикацией компрометирующих публичных постов от ее имени.

– Есть ли у Вас статистика: как много людей сталкивалось с кражей аккаунтов?

– За последний год с данной проблемой столкнулось 19% россиян. Довольно много на самом деле. При этом подавляющее большинство опрошенных не верят в то, что они могут быть интересны злоумышленникам.

Есть и другая не менее интересная статистика. Через Wi-Fi сеть 26% пользователей авторизуется в социальных сетях, а 41% хранит на своих устройствах логины и пароли. Каждый пятый респондент признался, что сообщает о себе слишком много информации в социальных сетях. Для людей, которые думают, что они находятся в защищенной среде, это нормально. Но на самом деле *интернет – сеть агрессивная и не безопасная. Поэтому там надо быть осторожными.*

Еще одна цифра – 35% фишинговых сайтов имитировали социальные сети. Речь идет о случаях, когда вам приходит какая-то ссылка, наподобие «посмотри я разместил интересный контент». Иногда контент создается специально для мужчин или для женщин. Мужчины больше реагируют на эротику, женщины – на общение, знакомства. Для них вирусописатели создают свои «завлекалочки», чтобы они кликали, переходили, смотрели.

– Какие пароли не стоит использовать в аккаунтах?

– Та же статистика свидетельствует о том, что *треть респондентов использует нестойкие ко взлому пароли. Самые популярные – «123456», «qwerty», «пароль», «откройся», «отвали».*

Но самые «хитрые» и «ловкие» люди используют *день рождения*. Они считают, что эту информацию точно никто не догадается посмотреть. Также легко можно узнать *номер телефона, имя и кличку животного*. Через это

обычно и взламывают. Вирусописатели получают информацию из разных источников, а зачастую мы сами размещаем ее в тех же социальных сетях.

– А откуда у Вас информация о самых популярных паролях? Неужели люди сами их Вам сообщали?

– Нет, это данные из реальных утечек бесплатных почтовых служб. Их анализировали, и в ТОП попали перечисленные.

– Мне доводилось слышать мнение, что значимая часть вирусного программного обеспечения попадает на наш компьютер вместе с - нелегальным софтом, который мы туда закачиваем. Так ли это?

– Надо понимать, что как только мы выходим на территорию нелицензионного, пиратского программного обеспечения риск значительно возрастает. Там злоумышленники гораздо активнее, а контроля правообладателей, наоборот, меньше. Я могу привести образный пример: если рыться в мусорном баке, то шанс подхватить инфекцию будет намного выше.

– А как с другими видами контента, например, с видео? Оно может нести в себе заразу?

– Само видео, как правило, нет. Но существуют всевозможные инструменты, с помощью которых видео оборачивается в определенные оболочки.

Другой вариант – пользователю предлагается формат avi, но на самом деле это может быть не видеоконтент, а исполняемый файл. Вирусописатели часто имитируют контент, подменяя его исполняемым файлом, который несет за собой вирусы. Может быть также предложен не контент, а просто ссылка.

Существуют случаи заражения через баннерную сеть с ресурсов, которые совершенно в этом не виноваты. Они просто подключили баннерную сеть, а через баннер предлагался определенный код, переход на который влек заражение компьютера.

– Андрей Юрьевич, можете дать один-два общих совета, как избежать самых серьезных угроз? Может быть, мыть руки перед тем, как сесть за компьютер?

– Мытье рук, конечно, поможет с точки зрения личной гигиены. Это никогда не лишнее. А вот *с точки зрения компьютерной гигиены самое важное – использовать лицензионное программное обеспечение и обновлять его*. Причем обновлять все программное обеспечение: не только операционную систему, но и установленный софт.

Кроме того, необходимо *использовать механизмы антивирусной защиты*. Все то, о чем я говорил, становится возможным, если вы не используете защиту. Это тот инструмент, без которого в сеть интернет выходить не стоит.

В момент, когда вредоносное программное обеспечение пытается проникнуть на ваше устройство, большинство антивирусных программ, программ фильтрации осуществят перехват. Это может происходить в терминальном режиме, и тогда вы даже не видите, что происходит. Но

программа ловит этот процесс, и спрашивает: вы действительно хотите это сделать?

– Вы говорите, что нужно регулярно обновлять программное обеспечение. Но ведь обновления могут быть фэйковыми.

– Безусловно, надо понимать, откуда пришло обновление. Если оно сброшено кем-то извне в виде ссылки, то этим пользоваться не стоит. Если же сам лицензионный продукт предлагает вам обновление, то этому источнику вполне можно доверять.

Приведу интересный кейс: так называемый Darkhotel. Эта ситуация из тех, в которые мы попадаем достаточно часто и, казалось бы, чувствуем себя достаточно уверенно. *Предположим, мы приезжаем в гостиницу и хотим подключиться к Wi-Fi*. Это вполне нормальное, естественное желание. При подключении запрашивается Wi-Fi сеть, которая может быть развернута злоумышленниками. Далее они предлагают для скачивания вредоносное программное обеспечение под видом обновления легитимного софта. Это может быть оболочка плеера, либо специальная утилита, которая работает специально для доступа в интернет только в этом отеле. А в действительности пользователь получает инсталлятор бэкдора, то есть открывает возможность закачивать стороннее программное обеспечение на свое устройство. Таким образом, злоумышленники получают возможность собирать информацию интернет-браузеров. Примечательно, что в настоящий момент данная угроза активна, она действительно присутствует в некоторых отелях. Это реально существующая беда.

– Какие еще полезные советы Вы могли бы дать?

– *У меня есть ТОП-10 советов:*

1. Заведите специальную карту для онлайн-покупок и не держите на ней большую сумму денег.

2. Не переходите на сайты по ссылкам в почтовых сообщениях, сообщениях в социальных сетях и чатах или кликнув по рекламному баннеру на сомнительном сайте.

3. Помните, что финансовые организации никогда не присылают писем с просьбой отправить им свои личные данные в электронном сообщении, перейти на сайт для авторизации или ввести личные данные во всплывающих окнах. Не переходите на сайт по ссылкам, присланным от имени банковских организаций и платежных систем.

4. Не переходите ни по каким ссылкам, присланным незнакомыми людьми.

5. Избегайте магазинов, зарегистрированных на бесплатных хостингах. Если сайт магазина вызывает сомнения, исследуйте данные о времени существования домена, на котором размещен сайт, и о его владельце на сервисах whois. Обратите внимание, на какой срок оплачен домен.

6. Внимательно анализируйте URL страницы с полями ввода конфиденциальных данных. Если интернет-адрес состоит из бессмысленного

набора символов или URL выглядит подозрительно, не оформляйте платеж на странице с этим адресом.

7. Проверяйте, используется ли при передаче ваших конфиденциальных данных шифрованное соединение. Если соединение защищенное, адрес сайта должен начинаться с https, а в адресной строке или строке браузера должна быть иконка закрытого замочка.

8. Вводите адрес банка или платежной системы вручную. Если вам пришла ссылка или даже если сайт сохранен в избранном, переходить на него все равно опасно. Вирусописатели всегда могут изменить эти ссылки, и неизвестно, куда вы попадете.

9. Старайтесь не пользоваться услугами онлайн-банкинга и не делать онлайн-покупки в публичных местах (интернет-кафе, клубах, библиотеках). На компьютерах могут быть установлены различные шпионские программы, считыватели нажатий клавиш, перехватчики интернет-трафика. Даже если вы пользуетесь своим компьютером, но при этом осуществляете банковские операции по публичной бесплатной сети Wi-Fi, существует риск перехвата трафика администратором этой сети, прослушивания посторонними лицами и атак с использованием сетевых червей, особенно если сеть Wi-Fi не защищена паролем.

10. Как я уже говорил, всегда держите операционную систему и антивирусное программное обеспечение в актуальном состоянии. Используйте на компьютере антивирусную программу с защитой от фишинга.

Не могу не сказать еще об одном интересном решении, которое недавно услышал от наших аналитиков. *Как защитить банковскую карточку на то время, когда я отдаю ее в чужие руки*, например, расплачиваясь в ресторане? Мне сказали: «Можно защититься циркулем». Я говорю: «Не понял, это как?». «Берешь циркуль и сзади трехзначный код аккуратненько стираешь». Дело в том, что когда мы отдаем карточку в чужие руки, злоумышленник одновременно получает и номер, и подтверждающий код на обороте карты. Эти три цифры можно или запомнить, или где-то записать.

– Какие угрозы в интернете, на Ваш взгляд, появятся в будущем?

– В первую очередь надо сказать о целевых атаках на банки. Мы видим, что этот тренд серьезен и количество атак будет расти.

Обязательно появятся новые уязвимости. С этим ничего не поделаешь, поскольку вирусописатели всегда находят огрехи любого кода.

Очень интересным обещает быть интернет вещей. Ваша кофеварка, холодильник и другие приборы будут сами заказывать себе расходные материалы. И вирусописатели наверняка попробуют использовать эти уязвимости в своих целях.

Ну и создание ботнетов под MAC – тоже вопрос ближайшего будущего.

О МОШЕННИЧЕСТВЕ С ЭЛЕКТРОННЫМИ ПОДПИСЯМИ

Источник: http://www.eos.ru/upload/analitica/Delo_2014-07_02.pdf

Автор: Наталья Храмцовская, к.и.н., ведущий эксперт по управлению документацией компании «ЭОС», эксперт ИСО, член Международного совета архивов

Описаны способы мошеннических действий с электронными подписями на документах – и это не всегда связано со взломом алгоритмов, есть достаточно обходных путей работы с «неопытными» владельцами ключей электронных подписей.

Противостоять мошенникам можно, лишь понимая их приемы, на этом мы и сосредоточились в статье. Особо отмечено, что нужно учитывать при долгосрочном архивном хранении электронных документов.

Кроме того, демонстрируются результаты нескольких экспериментов, в которых подписанный документ позже «меняет» отображаемую информацию, а электронная подпись на нем продолжает признаваться достоверной. Это впечатляет!

Технологии достаточно надежные, но...

Технологии электронных подписей и поддерживающая ее технология инфраструктуры открытых ключей имеют репутацию абсолютно надежных. В докладах нередко можно услышать, что их практически невозможно взломать. Но, как показывает практика, нет таких технологий,

которые мошенники тем или иным способом не смогли бы обернуть себе на пользу, – и именно на это хотелось бы обратить внимание в первую очередь. Это не первая технология, которая объявляется «пуленепробиваемой», и опыт уже показал, что не столько велика угроза возможных злоупотреблений при ее использовании (с которыми можно будет бороться), сколько опасна слепая вера общества и суда в надежность и непогрешимость данной технологии. Как следствие, пострадавшие от нового вида мошенничества люди могут сами быть заподозрены в мошенничестве и привлечены к ответственности.

Пример 1

В Великобритании при внедрении высокозащищенных банковских карт нескольких клиентов банков, первыми пострадавших от нового вида мошенничества и обратившихся за компенсацией, сначала отправили в тюрьму по обвинению в вымогательстве и лишь позже разобрались, что кражи совершали сотрудники банка.

Стоит также обратить внимание на то, что некоторые вопросы, связанные с предотвращением мошенничества с использованием электронных подписей, у нас не урегулированы законодательством, хотя уже имеется определенный зарубежный опыт. Негативную роль играет и то, что о проблемах и уязвимостях как-то не принято говорить открыто. Узкий круг специалистов в области информационной безопасности давно об этих проблемах знает, но вот широкие «народные массы» часто не в курсе того, что происходит. А тем временем сфера использования электронных подписей продолжает расширяться...

В мошенничестве с электронными подписями можно выделить 2 разновидности атак:

– Технические атаки, которые в основном направлены на взлом алгоритмов хеширования. В настоящее время такой метод мошенничества не слишком опасен, поскольку алгоритмы регулярно обновляются, но вот историкам и тем, кому предстоит обеспечивать долговременное хранение электронных документов, стоит обратить на него самое пристальное внимание. Есть лица, которые заинтересованы в искажении или подделке исторических документов, и для этого им достаточно взломать старые, созданные 20 и более лет назад алгоритмы, а это существенно более простая задача. Документы длительного срока хранения могут иметь значительную ценность, соответственно, последствия мошенничества могут быть серьезными.

– В настоящее время наиболее распространены другие методы мошенничества, связанные либо с обманом подписывающего документ человека, либо с кражей закрытых ключей. Кроме того, возрастают риски создания подставных аккредитованных удостоверяющих центров, способных выпустить квалифицированные сертификаты ключей электронных подписей без ведома людей, указанных в качестве их владельцев.

Существование и увеличение масштабов мошеннических действий с электронными подписями еще более усложняет проблему архивного хранения таких документов, поскольку архивам в своих стратегиях хранения придется учитывать риски подобного рода.

Доказательство компрометации алгоритма хеширования MD5 (2007-2008 гг.)

Технология электронных цифровых подписей использует метод ассиметричного шифрования, а также метод хеширования, который битовой строке произвольной длины ставит в соответствие битовую строку небольшой фиксированной длины, называемую хешем (дайджестом). Для этого разрабатываются специальные алгоритмы. В частности, алгоритм хеширования проектируется таким образом, чтобы вероятность коллизии – совпадения хешей двух различных строк битов, хотя теоретически и ненулевая, была бы настолько малой, что за разумное время с использованием самых мощных вычислительных систем сегодняшнего и

завтрашнего дня невозможно было бы подобрать другую строку битов, хеш которой совпадает с хешем известной строки битов. На практике это означает невозможность подобрать альтернативное сообщение, на которое можно «перенести» электронную цифровую подпись под известным сообщением так, чтобы она успешно проверялась.

Однако то, что один человек создал, другой всегда сумеет сломать. К настоящему времени ранние алгоритмы ЭЦП уже взломаны. Теоретическая возможность коллизий для алгоритма хеширования MD5, который первоначально широко применялся при создании электронных подписей (и до сих пор все еще используется в ИТ-отрасли для электронного подписания компьютерных программ), была доказана еще в 2004 году группой проф. Ван Сяоюнь (Xiaoyun Wang), однако многие считали эту угрозу не имеющей практического значения.

В 2007 году группа голландских специалистов – Марк Стивенс (Marc Stevens), Арьен Ленстра (Arjen Lenstra) и Бенне де Вегер (Benne de Weger) пообещала предсказать итоги выборов 2008 года в США и сообщила хэш-значение PDF-файла с предсказанием. На самом деле группа подготовила 12 (!) документов, 10 из которых позже были выложены в Интернете, имевших один и тот же MD5-хэш, – на все возможные (и некоторые невозможные) исходы выборов, см. Пример 2.

Пример 2.

Два из подготовленных документов: первый сообщает о победе на выборах Пэрис Хилтон, второй – о победе Барака Обамы (у всех документов один и тот же MD5-хэш: 3D515DEAD7AA16560ABA3E9DF05CBC80)

Эта эффектная демонстрация показала, что ЭЦП на основе алгоритма хеширования MD5 могут быть подделаны с использованием вполне доступного оборудования и сравнительно несложных программных инструментов.

Вот и получается, что электронная цифровая подпись, которую мы раньше знали под именем «ЭЦП», а теперь называем «усиленной электронной подписью», не так надежна, как кажется.

С одной стороны, по мере роста мощности компьютеров и развития математики алгоритмы устаревают и все хуже сопротивляются взлому, и очень беспокоит, что большинство коллег пока как следует не осознало последствия того, что электронные цифровые подписи все чаще используются при работе с документами длительного и постоянного срока хранения. У мошенников заинтересованность в подделке таких документов может сохраняться в течение длительного времени. К счастью, пока взлом алгоритмов требует специальных знаний и высокого уровня квалификации, которыми большинство людей не обладает.

При оперативной работе с документами можно не беспокоиться о такого рода уязвимостях, однако потенциальная возможность спустя длительное время изготовить «задним числом» и подложить в архив документы, электронные подписи под которыми будут успешно проверяться, должна тревожить тех, кому приходится работать с электронными документами длительного срока хранения.

С другой стороны, злоумышленники обычно идут по пути наименьшего сопротивления. Существуют другие, более простые и достаточно эффективные приемы, о которых и пойдет речь. Не случайно специалисты часто сравнивают электронную цифровую подпись со стальной сейфовой дверью, установленной в картонном домике. Чем ломать дверь, мошеннику проще или украсть ключи, или уговорить владельца самому ее открыть, или проделать дыру в картонной стене... Некоторые способы вполне по силам даже домохозяйкам.

Некоторые виды мошенничества, не требующие взлома алгоритмов

Наиболее распространенным способом мошенничества с электронными подписями является подписание подписью жертвы подложных документов или транзакций. В настоящее время несанкционированное списание денег через системы «клиент-банк» и интернет-банкинга приняло массовый характер. Как правило, доступ к ключевой информации осуществляется вследствие:

– небрежного отношения к хранению и уничтожению закрытых ключей;

– заражения вредоносными программами устройств, применяемых для подписания документов, а также использования злоумышленниками соответствующим образом «модифицированного» оборудования;

– подписания жертвой специально подготовленных документов, визуальное отображение которых может меняться.

Кроме того, сейчас стала реальностью еще одна угроза, связанная с возможностью создания подставных удостоверяющих центров, имеющих право выпускать усиленные квалифицированные электронные подписи.

Небрежное отношение к хранению и уничтожению закрытых ключей (ключей подписания)

К сожалению, у нас до сих пор среди тех, кто использует электронные цифровые подписи, хватает людей, не понимающих, что электронная подпись – не штампик и не факсимиле.

Пример 3

31.07.2007 приказом Министерства культуры и массовых коммуникаций РФ No 1182 был утвержден «Перечень типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения», который до сих пор действует. Полное непонимание технологии ЭЦП и правовых основ ее применения особенно ярко проявилось в пункте 1954 перечня, в котором для организаций одной из групп был установлен постоянный срок хранения для закрытых ключей ЭЦП.

Правовые последствия применения ЭЦП / усиленной электронной подписи (УЭП) базируются на том, что закрытый ключ (или, в терминологии закона «Об электронной подписи», ключ подписания) находится под полным контролем владельца ключа. Он никогда и ни при каких обстоятельствах не передается кому бы то ни было. Аннулированные закрытые ключи полагается как можно быстрее уничтожать, чтобы исключить возможность подписания электронных документов задним числом. Более того, для обеспечения максимальной безопасности лучше, чтобы ключевые пары создавались самим владельцем ключа и чтобы закрытый ключ никогда не попадал в чужие руки.

Постоянное хранение закрытого ключа, особенно если к нему есть возможность доступа посторонних лиц, обеспечивает идеальные условия для создания поддельных документов. В то же время закрытый ключ не используется в процессе проверки ЭЦП, поэтому хранить его не требуется.

Ряд нормативных документов как федерального, так и регионального уровня уже содержит (с некоторыми вариациями) требования об обязательном уничтожении закрытых ключей:

Фрагмент документа

Правила электронного документооборота в системе электронного документооборота Федерального Казначейства (из письма Федерального

Казначейства No 42-7.1-7/10.1-102 от 20.03.2007 «О примерном договоре «Об обмене электронными документами»)

4.2.7.12. После окончания срока действия Сертификата его владелец теряет право использования закрытого ключа подписи, соответствующего отзываемому Сертификату, и уничтожает указанный закрытый ключ подписи.

Фрагмент документа

Форма договора об обмене электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России, заключаемого между Банком России и клиентом Банка России (приложение к письму Банка России от 27.03.2013 No51-Т)

6.2. Клиент обязан:

6.2.6. Уничтожать закрытые ключи КА (ЭП) после истечения срока их действия.

С другой стороны, встречаются нормативные акты, согласно которым и уничтожение, и генерация закрытого ключа (ключа подписания) поручается сотрудникам удостоверяющего центра (УЦ) либо оператору информационной системы, что (за исключением случая использования высокозащищенных ключевых носителей, которые обеспечивают создание ключей внутри носителя и не допускают их передачу наружу) является грубейшим нарушением правил информационной безопасности при работе с ключевой информацией:

Фрагмент документа

Регламент удостоверяющего центра Федеральной службы по надзору в сфере образования и науки (утв. распоряжением Рособрнадзора от 18.12.2012 No4436-08)

15.3. Оператор УЦ на основании предоставленного заявления осуществляет уничтожение старой ключевой информации на ключевом контейнере, генерацию ключевых пар, запись закрытого ключа подписи на ключевой носитель, изготовление СКП ЭП (сертификат ключа проверки электронной подписи) и запись СКП ЭП на ключевой носитель.

Фрагмент документа

Регламент регистрации пользователей и поставщиков сведений и подключения их к государственной информационной системе миграционного учета (утв. приказом ФМС РФ No 38, МВД РФ No 91, Минкомсвязи РФ No 32, ФСБ РФ No 76, ФСТЭК РФ No 90 от 19.02.2010)

8. При подключении у пользователя и поставщика сведений АП (абонентских пунктов) или подключении АИС пользователя и поставщика сведений к информационной системе оператор информационной системы обеспечивает:

– изготовление, выдачу уполномоченным лицам пользователя и поставщика сведений, а также уничтожение ключей электронной цифровой подписи.

Если злоумышленник получает в свое распоряжение закрытый ключ, то надежность алгоритмов начинает играть против жертвы. Если электронная подпись успешно проверяется, то очень мало шансов на то, что впоследствии удастся доказать факт подписания документа неуполномоченным лицом и добиться возмещения понесенного ущерба.

Нарушение правил информационной безопасности при подписании электронных документов

Далеко не все понимают: надежность электронных подписей опирается на то, что процесс создания электронной подписи проходит в доверенной среде. Антивирусные компании регулярно оценивают масштабы заражения компьютеров, и на четвертой международной конференции Anti-fraud Russia 2013, прошедшей в ноябре 2013 года, сообщалось, что в России заражена половина компьютеров!

Вирусы сейчас все чаще пишутся под конкретное программное обеспечение, используемое для совершения банковских транзакций.

Подписание жертвой специально подготовленных документов, визуальное отображение которых может меняться

В последнее время у нас очень любят дискутировать на тему, что такое электронный документ. Коллеги из ИТ-сферы часто считают электронным документом любые данные, подписанные электронной подписью. Здесь, однако, есть одна тонкость, хорошо понятная специалистам, занимающимся управлением документами. Важнейшим качеством документа является его неизменность, причем не неизменность его как электронного объекта, а неизменность того, что отображается пользователю. Электронная цифровая подпись позволяет убедиться в неизменности электронного объекта, однако такой объект может представлять собой не только статические данные, но и содержать активный контент (встроенный код, макросы и т.д.), т.е. представлять собой программу, поведение которой может меняться. Достаточно в текст документа включить, например, макрос, показывающий при открытии документа текущую дату.

Эксперимент 1. Подписание PDF-файла, содержащего активный контент

Чтобы продемонстрировать риски, связанные с активным контентом, я провела эксперимент, в котором в PDF-файл был добавлен JavaScript-код (см. Рисунок 1), запрограммированный так, чтобы по истечении 10 минут документ стал нечитаемым – вместо текста отображался зеленый фон. После этого документ был подписан ЭЦП, поддерживаемой программой Adobe Acrobat.

Рисунок 1. PDF-документ со встроенным JavaScript-кодо

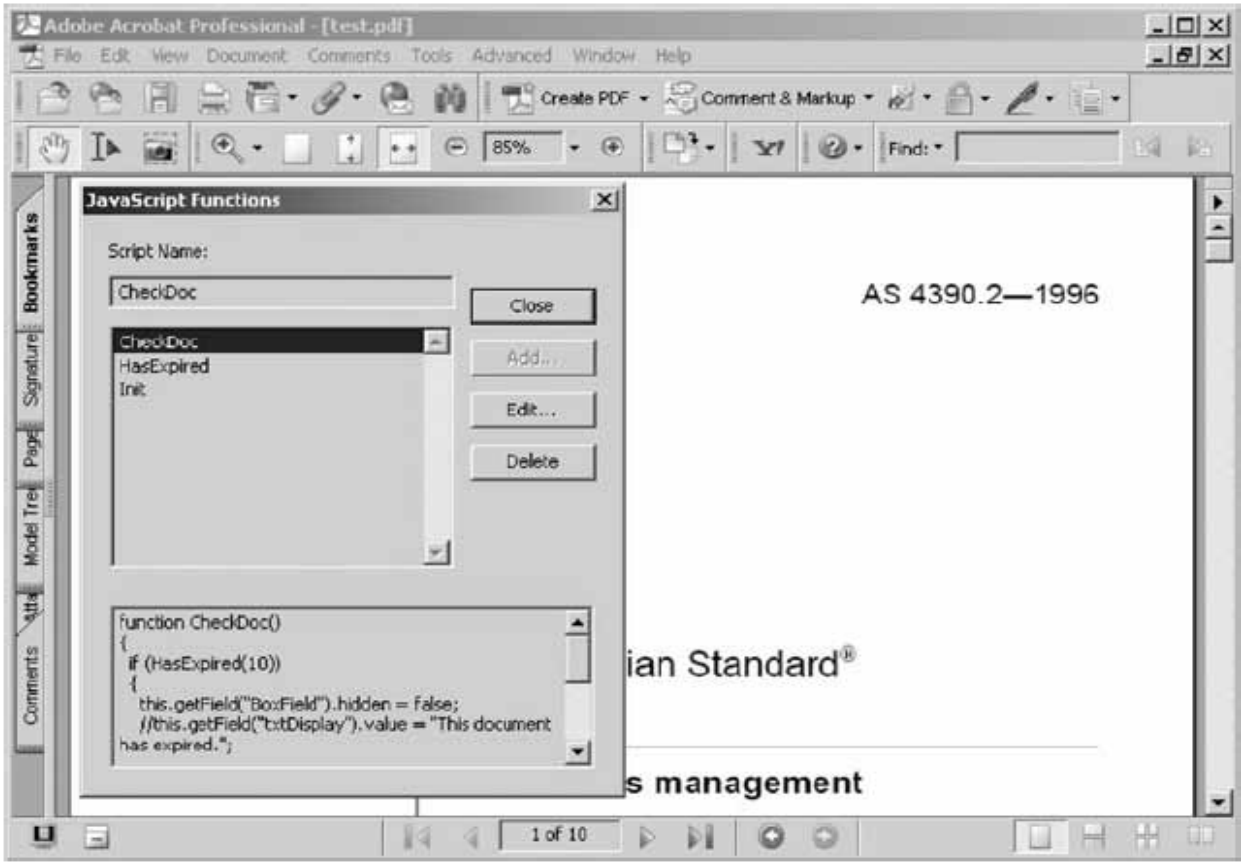
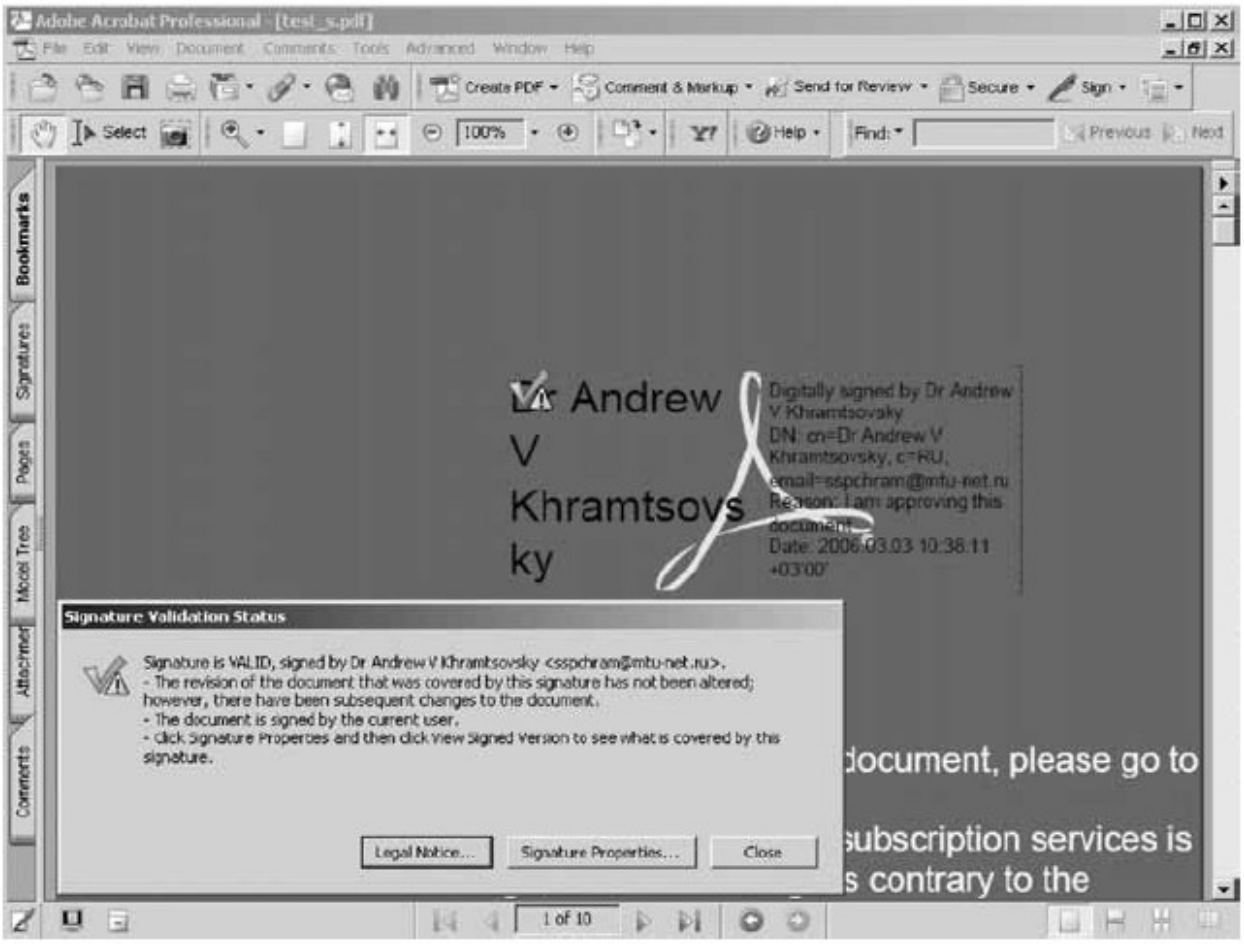


Рисунок 2. Проверка подписи спустя минуту – все хорошо, документ читается и подпись проверяется

Спустя минуту после подписания файл был снова открыт и была проведена успешная проверка подписи (см. Рисунок 2).

При попытке открыть файл через 11 минут его текст перестал отображаться, но при этом подпись проверяется и подтверждается ее подлинность (хотя Adobe Acrobat все-таки заподозрил, что дело не совсем чисто – он способен это сделать, поскольку «знает» внутреннее устройство документа), см. Рисунок 3.

Рисунок 3. Проверка подписи спустя 11 минут – текст не читается, но подпись проверяется



Недобросовестный контрагент вполне может прислать на подписание PDF-документ, который сегодня показывает один текст, а завтра – другой.

Зарубежный опыт минимизации рисков использования активного контента в электронных документах, подписанных ЭЦП / УЭП

В ряде стран для минимизации подобных рисков приняты меры на законодательном уровне. Так, устанавливается, что выявление встроенного кода в электронном документе приводит к возложению на того, кто его «подсунул» на подписание, обязанности доказывания его безвредности.

Наличие активного контента рассматривается как достаточное основание для того, чтобы отказать в принятии документа в качестве

доказательства. В нашем законодательстве подобных положений пока не содержится.

В законодательстве Австрии установлен явный запрет на использование активного контента:

Фрагмент документа

Указ Федерального канцлера Австрии об электронных подписях 2000 г. (в редакции 2004 г., параграф 4 п. 1) детализирует положения австрийского Закона об электронных подписях

Подписываться электронной подписью могут документы только в тех форматах, что рекомендованы поставщиком сертификационных услуг. Описания таких форматов должны быть общедоступны. Структура формата должна гарантировать неизменный вид документа как во время подписания, так и во время проверки подписи. Если формат допускает кодирование динамических изменений, то не разрешается использовать его элементы, вызывающие динамические изменения.

Согласно нормативной базе Италии выявление макросов или исполняемых кодов в электронных документах, подписанных квалифицированными подписями, приводит к тому, что такой документ теряет презумпцию подлинности и его подлинность приходится доказывать:

Фрагмент документа

Декрет Совета министров Италии от 13.01.2004 «Технические правила создания, передачи, хранения, воспроизведения, репродукции и проверки электронных документов» Электронные документы, подписанные цифровой подписью или усиленной электронной подписью иного вида, основанной на квалифицированном сертификате и созданной при помощи защищенного устройства для создания подписи, не создают эффекта, указанного в п. 3 ст. 10 [презумпция подлинности] сводного текста [Кодекса ЭП], если они включают макросы или исполняемый код, способные изменить представляемые документами акты, факты и данные.

Фрагмент документа

Декрет Совета министров Италии от 30.03.2009 «Технические правила создания, наложения и проверки электронной цифровой подписи» (пункт 3 статьи 3) Электронные документы, подписанные цифровой подписью или квалифицированной электронной подписью иного вида, не создают эффекта, предусмотренного п. 2 ст. 21 Кодекса [презумпция подлинности], если они включают макросы или исполняемый код, способные изменить представляемые документом акты, факты и данные.

В Словакии требования к файловым форматам документов устанавливают стандарты, выпускаемые Государственной службой безопасности, в которых также затрагивается данный вопрос.

Фрагмент документа

Требования к содержанию и формальные спецификации форматов документов, подписываемых усиленной электронной подписью, версия 1, Государственная служба безопасности (NBU) Словакии, 2007

При подписании и проверке подписанных усиленной электронной подписью документов необходимо, помимо самого подписания и проверки подписи, обеспечить также однозначную визуализацию подписанных документов.

Документ специфицирует транспортный формат для подписанных документов, роль которого заключается в обеспечении четкой идентификации типа подписанных документов для целей визуализации.

Документы-«перевертыши»

Еще один способ подделки электронного документа связан с использованием технических особенностей форматов. В ряде случаев один и тот же специально подготовленный объект в зависимости от его расширения может отображаться по-разному.

Эксперимент 2. В зависимости от расширения документ отображается по-разному

В 2007 году фирма NT Kernel Resources начала бесплатно распространять программу Merge Streams («Слияние потоков»), позволяющую слить в единое целое документ в формате Word и Excel-таблицу[1]. В зависимости от расширения файла виден или Word-документ, или электронная таблица. Если подписать такой файл ЭЦП / УЭП, то она в обоих случаях будет успешно проверяться.

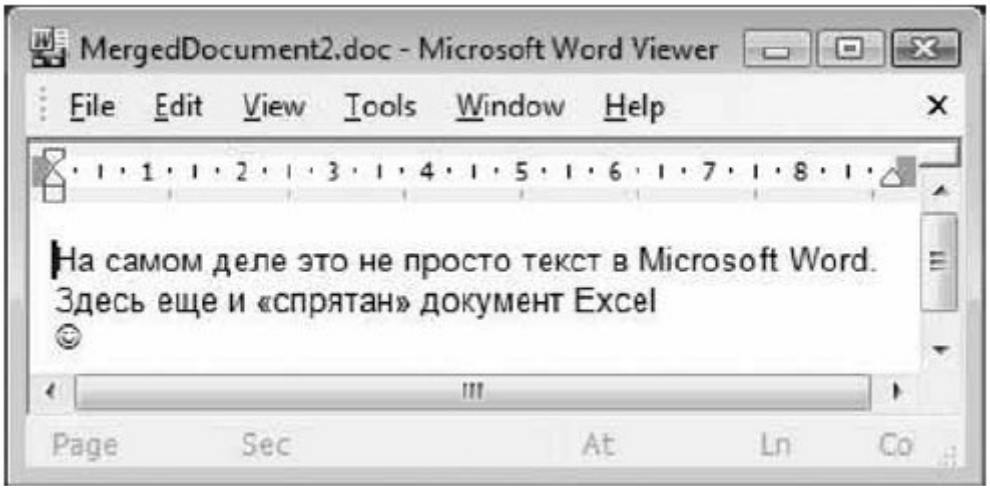
В 2008 году итальянские специалисты описали аналогичную атаку на статические форматы. Атака строится на создании «полиморфных» файлов, которые показываются по-разному в зависимости от расширения, и на том, что используемые ЭЦП не «покрывают» имя и расширение имени файла.

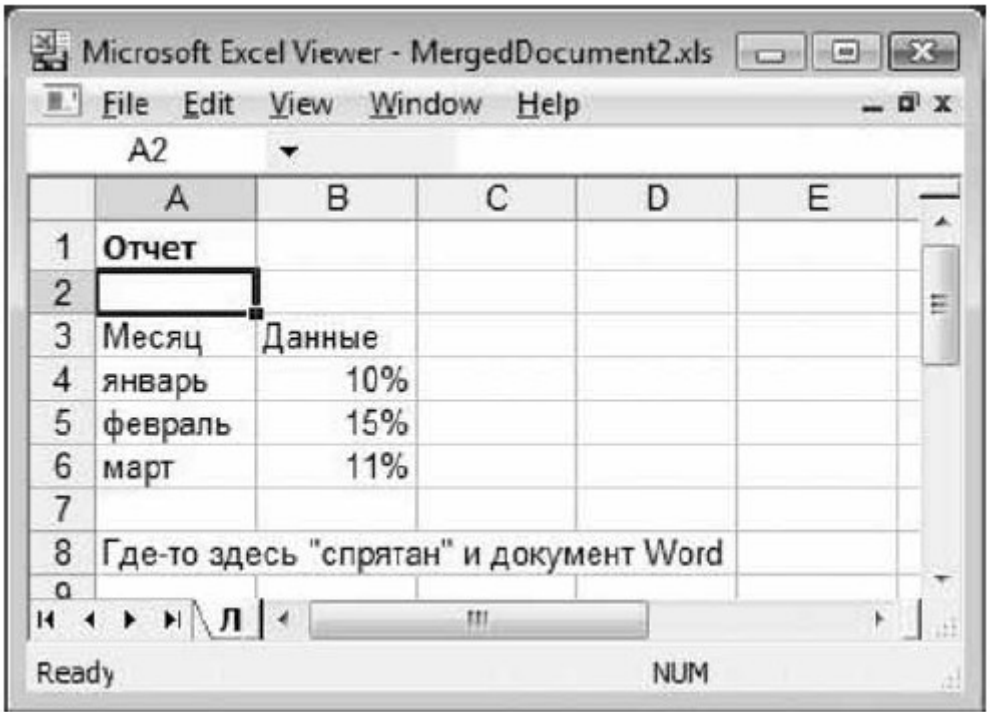
Франческо Буккафурри (Francesco Buccafurri) в ряде публикаций описал атаку на форматы BMP, TIFF, PDF. Независимо от него сходные результаты опубликовал чешский специалист Петер Рыбар (Peter Rybar).

Итальянское Национальное агентство по вопросам электронного правительства (CNIPA) признало уязвимость очень серьезной и заявило о том, что собирается предусмотреть контрмеры в очередной редакции итальянских правил применения ЭЦП.

[1] Андрей Подкин «Как спрятать документ на видном месте», 15 августа 2007 года, http://ecm-journal.ru/post/Kak-sprjatat-dokument-na-vidnom-meste.aspx.

Это один и тот же файл, однако в зависимости от расширения (.doc или .xls) он отображается по-разному:





Проверка усиленных квалифицированных подписей

При реальном использовании электронной подписи ключевую роль играет вся инфраструктура открытых ключей (PKI) в целом. И здесь наметились проблемы. Если в стране всего несколько аккредитованных удостоверяющих центров, то еще можно поверить в то, что они надлежащим образом проверены и сертифицированы. Однако в России аккредитованных удостоверяющих центров стало больше, чем в остальном мире. В «Перечень аккредитованных удостоверяющих центров», размещенный на сайте Минкомсвязи, по данным на 23.03.2014 внесено 338 удостоверяющих центров[2].

[2] См.: http://minsvyaz.ru/common/upload/Perechen_A_UZ_

Проблема здесь в том, что за вполне умеренные деньги можно создать и аккредитовать удостоверяющий центр, который в нужный момент «вбросит» квалифицированные сертификаты, выданные без ведома лиц, на имя которых они выданы.

Согласно закону все квалифицированные сертификаты равноправны, а созданные на их основе подписи приравнены к собственноручным. Жертвам потребуется немало времени и усилий на то, чтобы доказать, что это не их подписи. А тем временем злоумышленники, возможно, уже добьются желаемого результата. Именно ввиду этой угрозы неожиданно возрос интерес к неквалифицированным подписям, которые используются в рамках договорных отношений и сертификаты ключей которых выдаются одним или несколькими действительно доверенными удостоверяющими центрами.

Подводя итоги

Учитывая массовость распространения квалифицированных электронных подписей в нашей стране, можно сказать, что именно Россия является сейчас мировым лидером в их использовании, и в ряде случаев нам приходится первыми прокладывать дорогу.

В этих условиях необходимо критически относиться к технологии и понимать, что любой инструмент может быть использован не по назначению – не только во благо, но и во вред.

Важно сформировать разумное отношение к электронным подписям, такое же, как то, что давно сложилось в отношении «живой подписи». Как только люди осознают, что усиленные электронные подписи не являются стопроцентно надежными, они более активно начнут использовать другие технологии, как, например, простую электронную подпись.

Необходимо также внимательно отслеживать правоприменительную практику, выявлять «серые зоны» и оперативно дорабатывать законодательство в области использования электронных подписей.

Технология усиленных электронных подписей / ЭЦП уже продемонстрировала свою полезность и эффективность, но при этом у нее обнаружились и слабые места. С течением времени риск трудно обнаруживаемых атак будет лишь возрастать, поэтому работу с электронными подписями необходимо выстраивать таким образом, чтобы в максимальной степени этот риск снизить.

ПОЛОЖЕНИЕ О РОССИЙСКОМ СТРАХОВОМ ФОНДЕ ДОКУМЕНТОВ БИБЛИОТЕК (РСФДБ)

Источник: http://ifund.rsl.ru/assets/files/proekt.pdf

Настоящее Положение определяет назначение и состав российского страхового фонда документов библиотек, основные принципы его создания, порядок финансирования и материально-технического обеспечения работ по его формированию, хранению и использованию.

Положение разработано в соответствии с Постановлением Правительства Российской Федерации от 26 декабря 1995 No 1253-68 и вводится в действие с момента его утверждения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Российский страховой фонд документов библиотек (далее – РСФДБ) – это упорядоченная совокупность находящихся в государственной собственности Российской Федерации страховых копий документов библиотек, долговременно хранимых и надежно защищенных от уничтожения и разрушения. РСФДБ включает в себя сумму знаний, необходимых для обеспечения поступательного движения цивилизации при полной или частичной утрате фондов библиотек.

1.2. РСФДБ является частью Единого российского страхового фонда документации (ЕРСФД), создаваемого и используемого по установленным государством нормам и правилам.

1.3. РСФДБ создается с целью сохранения национального исторического, научного, культурного достояния и информационного ресурса страны в условиях чрезвычайных ситуаций, а также в случаях утраты документами их эксплуатационных свойств.

1.4. РСФДБ является федеральной собственностью, создается под руководством Министерства культуры Российской Федерации.

2. ОТБОР ДОКУМЕНТОВ ДЛЯ РСФДБ

2.1. Основными критериями отбора документов для включения в РСФДБ являются:

- непреходящая значимость для развития науки и производства;
- особая историко-культурная ценность;
- уникальность.

В определении очередности микрофильмирования документов учитываются их физическое состояние и активность использования. Приоритет отдается книжным памятникам (рукописям, редким книгам, газетам).

2.2. Отбор документов и направление их на микрофильмирование осуществляется в условиях координации и кооперации между

библиотеками Российской Федерации вне зависимости от ведомственной подчиненности.

2.3. Конкретные перечни документов, подлежащих микрофильмированию, формируются библиотеками с учетом данных Российского регистра страховых микрофильмов (далее – РРСМ), рассматриваются координационным методическим центром и согласовываются с Министерством культуры Российской Федерации

3. МИКРОФИЛЬМИРОВАНИЕ ДОКУМЕНТОВ

3.1. РСФДБ создается в виде рулонных микрофильмов документов, а именно: микрофильма рулонного (МР 35) на фотоплёнке шириной 35 мм по ГОСТ 13.1.104-93.

3.2. Изготовление микрофильмов РСФДБ производится:

- лабораториями микрофильмирования при библиотеках;
- лабораториями микрофильмирования других ведомств.

3.3. В соответствии с ГОСТ Р33.001-2006 при микрофильмировании документов изготавливаются черно-белые микрофильмы на галогенидосеребряных плёнках. Рекомендуемый комплект составляют:

• запасная страховая копия (МР 35 – негатив 1 поколения) – изготавливается в соответствии с требованиями ГОСТ 13.1.102-94 и передаётся на хранение в федеральную техническую лабораторию ЕР СФД;

• основная (архивная) страховая копия (МР 35 – негатив 2-го поколения) передается на хранение фондодержателю;

• пользовательская копия (МР 35 – позитив 3-его поколения) передается фондодержателю для оперативного использования.

3.3.1. Пользовательские копии микрофильмов изготавливаются посредством копирования основной страховой копии. Возможно изготовление пользовательской копии в виде электронного файла на основе сканирования основной страховой копии.

4. РОССИЙСКИЙ РЕГИСТР СТРАХОВЫХ МИКРОФОРМ

4.1. Российский регистр страховых микроформ (РРСМ) создается в целях:

- централизованной регистрации имеющихся микроформ;
- координации работы российских библиотек по отбору документов для страхового копирования;
- предоставления информации пользователям о библиотечных документах, переведенных на микроформы.

РРСМ представляет собой сводный каталог, отражающий сведения об изготовленных страховых копиях и переданных на хранение в федеральную техническую лабораторию.

4.2. РРСМ формируется на основе библиографической информации, своевременно предоставляемой библиотеками России в федеральный

методический и координационный центр для актуализации сводной базы данных.

4.3. РРСМ доступен всем библиотекам России, а также отечественным и зарубежным пользователям по телекоммуникационным каналам.

5. ХРАНЕНИЕ СТРАХОВЫХ МИКРОФОРМ

5.1. Хранение запасных страховых копий РСФДБ осуществляется в технической лаборатории ЕРСФД.

5.2. Основные (архивные) страховые копии хранятся в библиотеках, по заказу которых были изготовлены страховые микроформы, при соблюдении установленных стандартами условий хранения.

5.3. Организация-хранитель копий несет имущественную ответственность за соблюдение авторских и других прав правообладателей документов.

6. ИСПОЛЬЗОВАНИЕ МИКРОФОРМ

6.1. В процессе функционирования системы РСФДБ решается задача обеспечения доступности библиотечных фондов.

6.2. На основании Российского регистра страховых микроформ библиотеки Российской Федерации могут осуществлять заказ копий микроформ у библиотек, ответственных за изготовление страховой копии данного документа. Затраты на изготовление копий и их транспортировку оплачиваются заказчиком.

6.3. В случае утраты основной страховой копии или потери её потребительских качеств допускается по указанию Министерства культуры Российской Федерации изготовление новой основной страховой копии. Изготовление производится в технической лаборатории, где хранится запасная страховая копия за счёт средств организации – заказчика.

7. УПРАВЛЕНИЕ РСФДБ

7.1. Министерство культуры Российской Федерации осуществляет общее руководство созданием и функционированием РСФДБ, рассматривает проектные заявки, составляет сводные заявки (проекты плана) на создание РСФДБ.

7.2. ФГБУ «Российская государственная библиотека» (РГБ) является федеральным методическим и координационным центром по созданию РСФДБ. Функции и задачи РГБ как федерального методического и координационного центра по созданию РСФДБ включают:

- разработку проектов перспективных и годовых планов работ по созданию и сохранению РСФДБ;

- оперативное взаимодействие с поставщиками документации по вопросам представления документов для создания РСФДБ;

- взаимодействие с головными службами и организациями, находящимися в ведении других органов исполнительной власти по текущим вопросам;

- оперативный контроль выполнения работ по созданию и сохранению РСФДБ в соответствии с действующими нормативными документами;

- содействие работам по сертификации качества изготовленных страховых копий документов;

- оперативное взаимодействие с ФГУП «Научно-исследовательский институт репрографии», специальными и техническими лабораториями РСФДБ, а также с Министерством культуры Российской Федерации по текущим вопросам, возникающим в ходе работ по созданию, сохранению и использованию РСФДБ;

- ведение Российского регистра страховых микроформ;

- организационно-методическое и научное сопровождение работ по созданию и сохранению РСФДБ;

- отчетность перед Министерством культуры Российской Федерации за выполнение планов создания и сохранения РСФДБ;

- организацию выдачи страховых копий документов из страхового фонда по решению Министерства культуры Российской Федерации;

- подготовку и обоснование предложений Министерства культуры Российской Федерации по совершенствованию и развитию системы РСФДБ, а также материально-техническому и финансовому обеспечению ее функционирования;

- мониторинг деятельности библиотек в области страхового микрофильмирования;

- сотрудничество с ФГУП «Научно-исследовательский институт репрографии» в области создания РСФДБ в сфере нормативно-методической деятельности;

- анализ зарубежных источников, посвященных вопросам использования средств репрографии в целях обеспечения сохранности документов;

- микрофильмирование документов на базе собственных фондов РГБ или на базе документов, присланных библиотеками Российской Федерации;

- поддержка сайта, отражающего вопросы формирования страхового фонда библиотек Российской Федерации.

7.3. Библиотеки Российской Федерации разрабатывают перечни документов для создания РСФДБ, своевременно передают в РГБ библиографическую информацию для пополнения РРСМ, формируют заявки и представляют их в Министерство культуры Российской Федерации, осуществляют поставку комплектов документов для микрофильмирования в соответствии с планами создания РСФДБ,

обеспечивают заказ и получение необходимого количества копий, осуществляют заказ, получение и установку необходимых технических средств для работы с микрофильмами.

7.4. ФГУП «Научно-исследовательский институт репрографии» совместно с Министерством культуры Российской Федерации, Российской государственной библиотекой и библиотеками Российской Федерации разрабатывает необходимые нормативные и методические документы, обеспечивающие создание и функционирование РСФДБ, разрабатывает и контролирует технологические процессы создания РСФДБ.

7.5. Технические лаборатории осуществляют хранение запасных страховых микрофильмов и их копирование в случае утраты фондов библиотеками Российской Федерации.

8. ПОРЯДОК ФИНАНСИРОВАНИЯ РАБОТ ПО СОЗДАНИЮ РСФДБ

8.1. Работы, финансируемые Министерством культуры Российской Федерации в рамках ФЦП «Культура России»:

- микрофильмирование документов;
- передача на хранение в техническую лабораторию запасных страховых микрофильмов;
- хранение изготовленных и переданных в техническую лабораторию запасных страховых копий
- формирование российского регистра страховых микрофильмов;
- техническое оснащение и модернизация материально-технической базы лабораторий микрофильмирования при библиотеках, находящихся в федеральной собственности и предназначенных для создания документов РСФДБ;
- научно-методическое и нормативное обеспечение создания, сохранения и использования РСФДБ.

8.2. Затраты на сохранение основных страховых микрофильмов несут библиотеки в режиме планового бюджетного финансирования.

9. НОРМАТИВНАЯ БАЗА СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ РСФДБ

9.1. Нормативной базой создания, сохранения и использования РСФДБ являются государственные стандарты и руководящие документы классов 33 «Страховой фонд документации» и 13.1 «Репрография. Микрография».

ЕВРОСОЮЗ ОПРЕДЕЛИЛСЯ С ФОРМАТАМИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ И ПЕЧАТЕЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПОЛУЧЕНИИ ГОСУДАРСТВЕННЫХ ЭЛЕКТРОННЫХ УСЛУГ

Источник: Европейский правовой портал Eur-Lex
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_235_R_0006&from=EN

Недавно Евросоюз обновил своё законодательство по вопросам электронных подписей и услуг в области доверия, выпустив вместо реализуемых каждой страной через национальное законодательство европейской Директивы 1999/93/EC законодательный акт (Регламент) прямого действия (см. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG).

Теперь опубликован ещё один из предусмотренных регламентом подзаконных нормативных актов – «Исполнительное решение Еврокомиссии 2015/1506 от 8 сентября 2015 года, устанавливающее требования к форматам усиленных электронных подписей и усиленных печатей, признаваемых учреждениями и организациями государственного сектора в соответствии со ст. 27(5) и 37(5) утвержденного Европейским Парламентом и Советом Регламента № 910/2014 относительно электронной идентификации и услугам в области доверия для электронных транзакций на внутреннем рынке» (Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_235_R_0006&from=EN).

Регламентом было установлено, что в том случае, когда оказывающие электронные государственные услуги национальные органы и учреждения требуют использования усиленной электронной подписи и печати, то они обязаны признавать подписи и печати «определенных» форматов или альтернативных форматов, соответствующих конкретным требованиям. Исполнительным решением 2014/148/EU (см. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014D0148) был определен ряд наиболее широко распространенных форматов усиленной электронной подписи, работу с которыми страны-члены Евросоюза должны поддерживать для выполнения электронных административных процедур.

В приложении к новому решению перечислены существующие форматы усиленных электронных подписей. Это, в первую очередь, хорошо известные форматы:

- XAdES Baseline Profile (ETSI TS 103171 v.2.1.1, http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf),
- CAdES Baseline Profile (ETSI TS 103173 v.2.2.1, http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf) и
- PAdES Baseline Profile (ETSI TS 103172 v.2.2.2, http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf).

Из-за идущего процесса пересмотра органом по стандартизации вариантов электронных подписей для долговременной сохранности, эти варианты в данном решении не упоминаются.

РИЧАРД ПИРС-МОЗЕС: ЧТО НУЖНО ЗНАТЬ АРХИВИСТАМ?

Источник: сайт университета штата Джорджии в Клейтоне http://arstweb.clayton.edu/presentations/Pearce-Moses_GuerrillaApproach_ACA-UBC.pdf

Автор: Наташа Храмцовская

Недавно на сайте государственного университета Клейтон (Clayton State University), штат Джорджия, США, была выложена опубликованная в феврале 2015 года 8-страничная статья известного американского архивиста и педагога профессора Ричарда Пирс-Мозеса (Richard Pearce-Moses) «Партизанский подход к электронным архивам» (A Guerrilla Approach to Digital Archives), которая доступна по адресу http://arstweb.clayton.edu/presentations/Pearce-Moses_GuerrillaApproach_ACA-UBC.pdf .

Статья подготовлена по материалам доклада, сделанного автором 13 февраля 2015 года на 7-м международном симпозиуме «Профессиональное образование и архивы: Что понадобится в будущем?» (Professional Education and Archives: What Does the Future Require?) в Ванкувере, Канада. Симпозиум был организован студенческой секцией Ассоциации канадских архивистов (Association of Canadian, Archivists, ACA) при университете Британской Колумбии (University of British Columbia, UBC).

Ниже приведены несколько «выжимок» из этой статьи – надеюсь, они подтолкнут владеющих английским языком коллег к тому, чтобы прочесть эту публикацию в оригинале.

Что нужно знать архивистам?

Простой вопрос, отражающий основную тему данного симпозиума: что нужно знать профессионалам по работе с документами (специалистам по управлению документами, архивистам и т.д.) - особенно сегодня, с учетом того, что может потребоваться в будущем при работе с электронными документами и виртуальными архивами?

На данный вопрос, возможно, лучше всего ответить, дав ответ на второй вопрос: что делает, чем занимается архивист? Этот второй вопрос кажется простым, но меня часто поражают те ответы, которые дают на него архивисты – как студенты магистратуры в университете Клейтон, так и многих коллеги, которые уже много лет занимаются практической работой. Я не собираю статистику для анализа, но по памяти могу сказать, что наиболее распространенный ответ, который я получаю – это «Архивисты сохраняют прошлое» (или какой-либо похожий вариант, в котором использованы слова «память» или «история»).

Реже я получаю ответы типа «Архивисты хранят документы, которые защищают права и интересы граждан и организаций, а также помогают нам понять нашу культуру и историю». Это неплохой ответ, но на другой вопрос – он говорит о результатах, а не о самой деятельности.

В защиту коллег могу сказать, что данный вопрос часто застаёт их врасплох. В то же время, думаю, эти ответы свидетельствуют о том, что - на мой взгляд, и с точки зрения положения дел в США - знания и навыки многих архивистов основаны скорее на практике, чем на теории.

Более тридцати лет назад Фрэнк Берк (Frank Burke) бросил вызов профессиональному сообществу – четко сформулировать наконец, спустя пятьдесят лет после основания Общества американских архивистов, теорию архивного дела. Джон Робертс (John Roberts) ответил ему в своем эссе «Много шума о стеллажах»: «О чем тут можно теоретизировать?». Комментарии Робертса можно воспринять как антиинтеллектуальные, но они, как мне кажется, отражают прагматичное отношение, сформировавшееся у людей в «окопах», когда нужно было обеспечить, чтобы работа была сделана.

Лично я считаю, что существует достаточно простой ответ на вопрос о том, что делает архивист. Я часто поддразниваю затрудняющихся ответить на него своих коллег и студентов, говоря, что при этом вполне можно уложиться менее чем в 25 слов. Я опираюсь при этом на «Справочник», опубликованный Академией сертифицированных архивистов» (Academy of Certified Archivists), в котором перечислены основные виды деятельности архивистов:

- отбор, экспертиза ценности и прием на хранение;

- упорядочение и описание;
- справочная работа и обеспечение доступа;
- защита и обеспечение долговременной сохранности;
- информационно-пропагандистская работа и продвижение;
- управление архивными программами.

«Справочник» также отмечает, что профессионалам по работе с документами требуются основы общих знаний о природе документов и делопроизводстве, и им нужны специализированные знания из областей права и этики для того, чтобы направлять их деятельность.

Профессиональные теоретические знания

Архивисты по-прежнему нуждаются в профессиональных теоретических знаниях. Позвольте мне начать с примера. Когда-то в профессии был консенсус относительно того, что представляет собой документ. В электронную эпоху этот консенсус разваливается. Раздробленная на элементы информация в базе данных может быть собрана в несколько различных представлений. Являются ли эти представления документами? Являются ли они различными документами? Имеет ли значение виртуальность этих представлений, как в плане их нематериальности, так и в плане существования в виде потенциальной возможности воссоздания, а не сохраненных в зафиксированном виде? Где и что является документом – сами базы данных, различные представления или и то, и другое?

Архивистам нужно найти время, чтобы обдумать то, что ранее казалось очевидным, проанализировать и препарировать этот консенсус, и переосмыслить свое понимание того, что лежит в самой основе их профессии.

Вторым примером могут служить метаданные. Архивисты, как правило, думают о метаданных в связи с электронными документами. В прошлом мы обычно особо не задумывались о метаданных физических документов, потому что они были настолько привычными, что мы их не замечали.

Ещё один пример. Стандарт METS (Metadata Encoding and Transmission Standard – *стандарт кодирования и передачи метаданных – Н.Х.*), среди прочего, позволяет зафиксировать последовательность и взаимосвязь многих файлов, которые образуют единый документ. Для физических документов, их последовательность и взаимосвязь может быть зафиксирована при помощи физических метаданных в виде скобы или скрепки.

Я использую подобные примеры для того, чтобы показать, какие теоретические знания необходимые для специалистов по работе с документами в электронную эпоху. Практически для каждого аспекта архивной работы необходимо провести аналогичный анализ, чтобы в полной мере понять, с чем же мы имеем дело. Я также заметил, что многие - если не все – проблемы, с которыми я сталкивался при работе с электронными

документами, имели свои аналоги в мире физических документов, способствующие пониманию вопроса и подсказывающие новые решения.

Технические знания и навыки, нужные представителям нашей профессии

Помимо понимания теории профессии, архивисты должны обладать знаниями технологий и электронной информационной экосистемы. Какие же технологии архивистам следует знать?

Во-первых, нужна общая эрудиция и умение свободно обсуждать эти вопросы. Наши выпускники должны быть в состоянии вести осмысленный разговор с ИТ-специалистами. Они должны уметь формулировать свои потребности на понятном ИТ-специалистам языке. Они также должны понимать специалистов по технологиям, которые приходят за стол совместных обсуждений, имея собственное видение мира и язык. В ходе коллективной работы представители каждой из профессии высказывают свои предложения, касающиеся решаемой задачи. Архивисты должны быть способны воспринимать предложения, делаемые ИТ-специалистами - предложения, которые могут представлять собой хорошую практику в корпоративной среде, но могут не соответствовать специфическим потребностям архивов.

Во-вторых, архивистам нужны базовые компетенции - какое-то количество технических знаний и навыков, достаточное для выполнения обычных рутинных операций. Они не должны рассчитывать на то, что у них будет возможность привлечь ИТ-специалистов для выполнения всей чёрной работы с электронными документами. Напротив, я считаю, что архивисты должны уметь манипулировать и управлять электронными документами точно так же, как они манипулируют и управляют физическими документами.

Наконец, я считаю, что опытные архивисты в электронную эпоху будут уметь общаться и владеть знаниями и навыками на продвинутом уровне. Очень немногие выпускники выйдут из вуза, имея подобный уровень подготовки. Скорее всего, у них будет солидная теоретическая и техническая база, на основе которой они смогут расти. Настоящими профессионалами они станут после нескольких лет практической работы, включающей в себя изучение всё большего и большего числа новых инструментов и экспериментирование с ними. Со временем они освоят многие из навыков профессиональных ИТ-специалистов.

АВСТРАЛИЯ: ПОЛОЖЕНИЕ ДЕЛ С ХРАНЕНИЕМ ФИЗИЧЕСКИХ ДОКУМЕНТОВ В ГОСУДАРСТВЕННЫХ ОРГАНАХ ШТАТА ВИКТОРИЯ

Источник: сайт PROV http://prov.vic.gov.au/government-recordkeeping/research-into-physical-record-storage-within-victorian-government

Начиная с 2013 года, Управление государственных документов австралийского штата Виктория (Public Record Office Victoria, PROV) провело ряд обследований с целью определить объемы, местонахождение и расходы на хранение физических документов органов исполнительной власти штата, хранимых ими как у себя, так и в коммерческих центрах хранения.

Хотя наше исследование продолжается, уже появился ряд наблюдений, которыми мы можем поделиться.

Рост объёмов физических документов не прекратился

Несмотря на активизацию усилий по оцифровке, мы по-прежнему наблюдаем устойчивый рост объёмов хранения физических документов. По нашим оценкам государственные органы штата хранят в общей сложности 800 погонных километров документов (*по нашим меркам, это примерно 32 миллиона стандартных дел*), содержание которых ежегодно обходится в миллионы австралийских долларов.

Иногда нам в неофициальном порядке объясняют, почему государственные органы неактивно занимаются уничтожением документов. В одном из случаев причиной является высокая, уплачиваемая авансом стоимость уничтожения стандартного архивного короба в коммерческом центре хранения, равная стоимости года хранения того же короба.

Тем не менее, выполнение программы уничтожения документов с истекшими сроками хранения не только обеспечивает исполнение государственными органами своих обязательств в области управления документами, но в долгосрочной перспективе позволит реально сэкономить деньги, снизить бремя административных расходов и сдержать рост объёмов физических документов.

Без нужды одновременно хранятся бумажные оригиналы и их электронные копии

Ещё в одном государственном органе нам рассказали о том, что во многих случаях, по завершении проекта оцифровки, сохраняются как исходные бумажные документы, так и их электронные копии.

Это не только лишает государственные органы мотивации проводить дальнейшие проекты по оцифровке, но и приводит к дополнительным административным расходам. Порой имеются законные основания для

использования такого подхода, когда, например, бумажный подлинник ценен как физический артефакт или если существует нормативное требование о сохранении документов в определенном формате. Однако во многих случаях существует путаница и непонимание относительно того, когда исходные документы могут быть уничтожены после преобразования в другой формат.

Согласно Руководству по использованию Типового перечня для преобразованных исходных документов (Guide to the GDA for converted Source Records, http://prov.vic.gov.au/wp-content/uploads/2015/01/1001G1v1.3.pdf), государственным органам рекомендуется сначала накопить опыт работы по проведению конверсии, связанной с низким риском, прежде чем приступать к более рискованным масштабным конверсиям.

Вероятнее всего, Вам потребуется подготовить деловое обоснование с целью получения поддержки и ресурсов для Ваших проектов оцифровки и хранения. Управление государственных документов штата подготовило полезное Руководство по написанию делового обоснования (Writing a Business Case Guideline, http://prov.vic.gov.au/wp-content/uploads/2012/04/PROS1010-G4-v2.0.pdf), которое может быть использовано для представления Вашего проекта или инициативы, получения одобрения и финансирования. В дополнение к этому, Вас также может заинтересовать «калькулятор отдачи» (impact calculator), доступный по адресу http://www.jiscinfonet.ac.uk/tools/impact-calculator/

ФРАНЦИЯ: ПОДТЕКАНИЕ ТРУБОПРОВОДОВ В ХРАНИЛИЩЕ НАЦИОНАЛЬНЫХ АРХИВОВ В ФОНТЕНБЛО

Источник: сайт издания «La République»
http://www.larepublique77.fr/2015/08/03/fontainebleau-archives-nationales-inondees-fleur-pellerin/

Подтекание трубопроводов было зафиксировано в пятом полуподвальном хранилище филиала Национальных Архивов Франции в Фонтенбло (Fontainebleau). Плохой знак – за несколько месяцев до принятия министром культуры Флёр Пеллерен (Fleur Pellerin) решения о будущем филиала.

Новая катастрофа произошла в многострадальном филиале Национальных Архивов Франции в Фонтенбло. В то время, как его здание по-прежнему закрыто из-за серьезных проблем с устойчивостью конструкций (см. http://www.larepublique77.fr/2015/06/18/alerte-rouge-sur-les-archives/), а

решение о его будущем до сих пор не принято, - 15 июля 2015 года была зафиксирована протечка в 5-м хранилище.

В течение лета в филиале будут проведены работы по диагностике его технического состояния, что позволит министру культуры принять свое решение. Ясно, что это в первую очередь будет вопрос о том, возможно ли его отремонтировать или нет. Для этого два месяца будут сниматься показания с устройства измерения трещин, с целью определить подвижки в конструкции здания. Как пояснил заместитель директора Национальных Архивов Николя Узело (Nicolas Houzelot), «Мы обнаружили протечку в ходе этих технических работ. Вода бала откачана, и мы предприняли срочные меры. К счастью, никакие документы не были уничтожены, но мы обнаружили присутствие плесени». Таким образом, короба покрылись плесенью, но по мнению руководства, содержащиеся в них материалы вполне можно сохранить. Мы говорим здесь о массиве в 33 тысячи документов!

Сотрудники хотят поговорить с Флёр Пеллерен

Это было первое посещение 5-го хранилища с марта 2014 года. Чтобы решить проблему, в ближайшие дни будут установлены промышленные осушители воздуха. «Сейчас каждая проблема становится ещё сложнее из-за рисков, связанных с неустойчивостью здания», - признает г-н Узело. Между тем, сотрудники, которые и так уже были в напряжённом состоянии, встревожены: «Ситуация в филиале не только не улучшится, но на самом деле становится еще хуже», - говорится в их заявлении. «Возможность причинения ущерба документам можно было предвидеть с самого начала, и, к сожалению, с марта 2014 года здания не обслуживаются и не охраняются. Мы осуждаем ожидающую историческую память нашей страны масштабную катастрофу для культурно-исторического наследия и архивного дела, которая сведёт на нет многие годы работы».

На самом же деле протечка не повлияет на судьбу филиала в Фонтенбло. Работы по технической диагностике были задержаны на восемь дней: «С одной стороны, нам удалось справиться с ЧП в виде подтопления», - подводит итоги г-н Узело. «С другой стороны, мы пытаемся решить проблему устойчивости здания, и я не могу предсказать, какие решения будут приняты». Принятие решения, очевидно, станет уделом министра культуры Флёр Пеллерен. Сотрудники филиала, написавшие о своём бедственном положении президенту страны Франсуа Олланду, надеются на то, что министр в ближайшее время встретится с ними. Спорить, наверное, будет напрасно, потому что судьба филиала «у прекрасного фонтана» (*так можно перевести «Фонтенбло»*), как никогда ранее, находится под вопросом.

ЗМІСТ