



ПЕРЕДМОВА

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

У публікації «Есть ли будущее у микрографии» наведено переклад провідного інженера-технолога НДІ мікрографії Журавля О. Г. виступу виконавчого директора американської компанії Analogue Imaging LLC Арона Баркела про можливості використання мікрографії у 21-му віці на засіданні круглого столу в м. Казань, квітень 2018 року.

У публікації «Информационная безопасность предприятия: теоретико-методологические основы правового обеспечения» розглянуто проблему забезпечення інформаційної безпеки підприємства як суб'єкта інформаційного права та інформаційних правовідношень.

У публікації ««Режим конфиденциальности» электронной почты Gmail» розглянуто новий «механізм забезпечення конфіденційності» пошти Gmail, який дозволяє зберігати контроль над повідомленням та, відповідно, надає можливість ефективно блокувати доступ. Наведено можливі наслідки для архівної справи.

У публікації «Франция: Опубликован порядок оказания услуг «электронного сейфа»» розповідається про прийнятий у Франції Кодекс поштових послуг та електронних комунікацій, який надає можливість зберігання окремими особами та організаціями своїх електронних документів без зменшення їх правової та доказової сили та визнаних законодавством.

У публікації «Конференция Инфодокум-2018 «Цифровая экономика»» розповідається про питання, які було розглянуто на конференції.

У публікації «ИСО: Готовится стандарт PDF/R для хранения и передачи растровых изображений» розповідається про формат PDF/Raster який розроблено для використання в якості стандартного формату зберігання, передачі та розповсюдження відсканованих документів.

У публікації «Штат Виктория, Австралия: Онлайн-решение ORDA для разработки и актуализации указаний по срокам хранения и действиям по их истечении» розповідається про рішення ORDA для підтримки в онлайн-режимі розробки, надання на затвердження, публікації та подальшої актуалізації вказівок по термінам зберігання документів та діям по закінченню терміну їх використання.

У публікації «ИСО: Технический отчет по микроклимату среды хранения архивно-библиотечных материалов» надано інформацію про зміни у рекомендаціях та посібниках з управління навколишнім середовищем під час збереження культурно-історичної спадщини.

У публікації «Консорциум Всемирной паутины W3C выложил проект пересмотренной версии публикации «Недостатки САРТСНА в плане обеспечения доступности»» розповідається про оновлену редакцію автоматизованого публічного тесту Тьюринга для розрізнення комп'ютерів і людей.

У публікації «У публікації «Фонд «Открытая сохранность» опубликовал свою новую стратегию на 2018 – 2021 годы» розповідається про нову стратегію, яка дозволяє організаціям оцінювати, перевіряти, документувати, пом'якшувати ризики і обробляти підлягає збереженню електронний контент відповідно до бажаними політиками і передовим досвідом спільноти.

У публікації «Хорватия: Принят новый закон об архивных материалах и архивах» розповідається про новий закон, який забезпечить створення, збереження і конвертацію документальних і архівних матеріалів в цифровій формі.

У публікації «Евросоюз: Опубликованы новые стандарты семейства LOTAR» розповідається про нові опубліковані документи в рамках роботи над стандартом EN 9300 «Забезпечення довготривалого збереження і можливості використання електронної документації на технічні продукти, такий, як 3D-моделі, дані САПР і PDM-систем, в аерокосмічній галузі».

У публікації «Новая эра сотрудничества в проведении исследований в области обеспечения долговременной сохранности электронных материалов» розповідається про проект, який повинен об'єднати зусилля в області досліджень компаній Arkivum і Фонду «Відкриті збереження». Результатом може стати початок нової ери спільних досліджень, що проводяться всіма новаторами в області електронного збереження.

У публікації «Национальные Архивы Великобритании тестируют использование блокчейна для целей обеспечения долговременной сохранности исторических документов» розповідається про дослідження з метою використовувати технологію блокчейна для того, щоб унеможливити внесення несанкціонованих змін в історичні документи.



ЕСТЬ ЛИ БУДУЩЕЕ У МИКРОГРАФИИ

Источник: <http://rusrim.blogspot.com/2018/05/1.html>

Перевод: А. Г. Журавля – ведущего инженера-технолога НИИ микрографии

На круглом столе проходившем в рамках Международной научно-практической конференции «От пергамента к цифре», г. Казань, 18 – 20 апреля 2018 г. прозвучал вопрос: «Есть ли будущее у микрографии, в какой форме (электронно-цифровая или аналоговая запись информации) она будет использоваться?».

Отвечая на него, исполнительный директор американской компании Analogue Imaging LLC Арон Баркел высказал очень интересную точку зрения и дал достаточно объективную оценку возможности использования микрографии в 21-м веке.

Выступление Арона Баркела

Вы знаете, интересно анализировать с технологической и цифровой точки зрения то, что произошло за последние 30 лет. Было высказано утверждение, что время микрофильма давным-давно ушло. Существует одна, на мой взгляд, уникальная причина, по которой микрофильм до сих пор не вышел из употребления, – чтобы его прочесть, нам всего лишь нужны свет, увеличение, и наши глаза. И чтобы прочесть такую информацию, нам не нужна крупная прибыльная компания. Вот по этой причине, на мой взгляд, и продолжается микрофильмирование.

Хочу поделиться с Вами информацией о том, что в США есть два штата, которые решили прекратить микрофильмирование и убрали соответствующую информацию из своей юридической литературы. Оба этих штата пытались хранить информацию в цифровом виде. Оба этих штата потеряли записи и, потерпев неудачу, вернулись, скажем так, к чертежной доске.

Если эффективность нашей работы по сохранению данных составляет 99%, значит нам нужно 100%. Когда мы говорим о критически важных документах, таких как записи о рождении, о смерти, о браке, мы говорим о людских историях, и всякий раз, когда я думаю о документе, я всегда стараюсь думать и о документах, подобных моим личным записям.

Когда я принимаю решение о том, как я собираюсь хранить записи о рождении своих детей, как мне хранить самые важные для меня записи, и, как я уже сказал, у нас есть штаты, которые вернулись к чертежной доске, упомянув технологию микрофильмирования, как действительно старую и архаичную, мы до сих пор ее используем.

Я всегда возвращаюсь к найденным нами первым микроформам времен Крымской войны. Эти микроформы до сих пор читаются. Вы можете прочесть эти микроформы и сегодня. Несмотря на то, что Крымская война

была давно, это полноценный архив, которому более ста сорока лет, и он может быть ее доказательством.

Итак, когда вы спрашиваете, есть ли будущее у микрофильмирования, я полагаю, что мы можем ответить на этот вопрос утвердительно, по крайней мере, относительно моей страны, когда ошибки, допущенные при цифровой записи, привели к потере данных, и система дала сбой.

Мы говорим об облачных хранилищах. Хорошо знаю, что слово «облако» звучит приятно, но что оно представляет собой на самом деле? Это куча серверов, которые могут сбоить, выйти из строя. Возможна нацеленная атака с целью нанести ущерб вашим данным со стороны того, кто может быть вашим недоброжелателем.

Я полагаю таким образом, что вы знаете, почему я думаю, что микроформа будет существовать.

По моему мнению, есть чрезвычайно ценные базы данных по всему миру, одна из этих ценных баз данных – данные о переписи населения Соединенных Штатов. Для нас перепись населения Соединенных Штатов не только ведется в цифровом формате, но и хранится на пленке в совершенно разных местах.

Вы все здесь говорите о юридическом аспекте этих записей, которые мы предоставляем. Существует некоммерческий кооператив библиотек, называемый Law Library Microform Consortium (LLMC). Деятельность этой организации состоит в сохранении юридических титулов и правительственных документов.

У них есть правовые документы, касающиеся 90% юридических лиц. Университеты и все те, кто хранят свою историю в цифровом виде, могут также иметь ее в микрографической форме в двух разных местах.

Эти варианты, на мой взгляд, являются самым безопасным способом сохранить записи.

Опять немного возвращусь к гибриднему подходу, имеющему несколько разновидностей записи. Мой совет государственным архивам и федеральным архивам в Соединенных Штатах: почему бы вам не сохранять данные на бумаге, микроформе или в какой-либо другой удобочитаемой для человека форме? Таким образом, вы можете позволить себе использовать как цифровую, так и аналоговую технологию, чтобы, скажем так, понять лучший путь ее применения.

Возможно, у вас есть носитель, которому более четырех лет, и приходит время его замены. Когда я говорю «носитель», то подразумеваю, как мы храним цифровые данные.

У жестких дисков или серверов ресурс работоспособности не бесконечен. Вы знаете также, что они постоянно совершенствуются, становятся все быстрее и лучше, но у них нет единого стандарта, и поэтому я думаю, что микрофильм будет существовать.

В последнее время новые технологии приходят в наш мир по-настоящему быстро, и микрофильм в этом плане не является исключением.

Сейчас автоматическое распознавание изображений с использованием микрофильма – обычное явление. Выполняется также запись и воспроизведение бинарных данных с использованием микрофильма и штрихового кодирования. Это весьма перспективно.

Выполняется цветоделение с записью на микрофильм и последующее восстановление из микрофильма обратно в цветное изображение на черно-белой пленке.

Что я хочу этим сказать? Существует много современных цифровых технологий, и каждый из вас вправе задать вопрос: давайте откажемся от микрофильма, потому что в цифровом виде все выполняется точно и быстро, а для получения микроформы требуется так много времени.

Люди просто не знают современных технологий микрофильмирования.

Хочу сказать, что в США микрофильмирование есть во всех штатах. Все штаты и графства имеют определенный закон, который гласит, что если запись старше X лет, она должна храниться или в бумажной форме, или в микроформе.

В заключение, хочется сказать об очень важной вещи, которую нужно принять во внимание, если вы действительно хотите серьезно относиться к своему архиву, и ваши записи важны для вас.

По моему личному убеждению, ум и сообразительность играют важнейшую роль в истории, и, возвращаясь к началу моего ответа, повторю: у нас есть глаза, у нас есть Солнце, у нас есть увеличительное стекло. Не нужно контролировать все эти постоянно меняющиеся стандарты, ведь мы всегда можем получить нашу собственную информацию с микрофильма.

Участники конференции прокомментировали выступление Арона Баркела:

1. «Существует, по крайней мере, одна компания в мире, которая использует микрофильм для хранения цифровой информации. Они хранят биты и байты на микрофильме, поэтому, на мой взгляд, реальный вопрос заключается не в том, что мы используем микрофильм, а насколько надежны посреднические устройства, потому что то, что вы действительно хотите достичь, – это хранить информацию на носителе высокой плотности, который не нуждается в распознавания при чтении.

И с этой точки зрения первая проблема заключается в том, что не будет достаточного количества компаний для производства микрофильмов, в первую очередь, самой пленки как носителя. Но тогда, если кто-то изобретет простой носитель, который позволит нам читать информацию очень дешево, это станет отличной альтернативой микрофильмам. Однако я считаю, что реальной проблемой является надежность устройств сопряжения, потому что, как вы сказали, программное обеспечение устаревает, поэтому риск потери информации весьма велик».

2. «Возвращаясь к гибридной среде, я хотела бы добавить кое-что к вышесказанному. Есть огромное количество записей, которые по закону мы

должны хранить в течение очень долгого времени, хотя они имеют слишком громоздкий вид. Если бы такие записи были в цифровой форме, нам приходилось бы переводить их на следующую систему каждые три-пять лет. Это большие денежные расходы. А если это микрофильм, то Вы просто убираете его на сто лет туда, где Вы должны его хранить.

В случае запроса какого-либо микрофильма, его всегда можно прочитать, используя увеличительное стекло. Поэтому я полностью поддерживаю такой способ записи».



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ: ТЕОРЕТИКО- МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ

Источник: <http://applaw.knu.ua/index.php/arkhiv-nomeriv/4-6-2013/item/240-informatsionnaya-bezopasnost-predpriyatiya-teoretiko-metodologicheskie-osnovy-pravovogo-obespecheniya-nashinets-naumova-a-yu>

Автор: Нашинец-Наумова А. Ю

Статья посвящена проблеме обеспечения информационной безопасности предприятия как субъекта информационного права и информационных правоотношений. Под информационной безопасностью предприятия понимается сохранение в тайне коммерчески важной информации, позволяющей успешно конкурировать на рынке товаров и услуг.

Предприятие – это инструмент удовлетворения потребностей и достижения определенных целей общества, социальных групп и индивидов. Эффективная деятельность предприятия предполагает, что она обеспечивает безопасность своих членов, выступает средством выживаемости человека, действующего в ее рамках. В тоже время само предприятие подвергается разнообразным опасностям, угрожающим ее существованию и целостности. Это обуславливает необходимость обеспечения деятельности по повышению защищенности жизненно важных интересов предприятия и её членов.

Проблема информационной безопасности предприятия, являясь проблематикой, как общей теории организации, так и информационного права, сегодня приобретает новые аспекты. Их появление предопределяется в первую очередь качественными изменениями самого социума и его внешней среды.

Человек в стремлении повысить степень своей защищенности от негативного воздействия природных сил так изменил условия своего

существования, что они сами стали источником опасностей. Развитие общества, научно-технического прогресса со всей ясностью показывает, что среда обитания человека отнюдь не обладает такими качествами, как прозрачность, определенность, стабильность, что характерно для состояния безопасности в целом и информационной безопасности в частности. Наоборот, сегодня ей присущи противоположные по своему содержанию характеристики, что спровоцировало новый виток в деятельности по обеспечению безопасности. Это предполагает новый уровень в разработке как теоретических вопросов информационной безопасности, так и практических мер по ее обеспечению.

Сегодня наблюдается повышенное внимание представителей всех социальных наук к тематике информационной безопасности. Необходимо отметить работы А. Баранова, К. Белякова, В. Брижко, И. Гаврилова, М. Гуцалюка, Л. Задорожной, А. Зинченко, Г. Лазарева, Д. Ловцова, А. Марущака, А. Новицкого, Р. Северин, В. Цымбалюка, Н. Швеца и др. Последнее время подготовлен ряд диссертационных исследований, посвященных вопросам информационной безопасности, при этом следует отметить, что большинство этих работ связано с вопросом информационной безопасности государства или обеспечения безопасности информационных систем. Однако проблема информационной безопасности предприятия остается недостаточно исследованной. Это связано в частности с тем, что авторы больше внимания уделяют обеспечению информационной безопасности государства, а также с отсутствием целенаправленного подхода к проблеме в целом у тех ученых, которые затрагивали роль информации в деятельности предприятия. Поэтому автор в данной работе пытается проанализировать вопросы обеспечения информационной безопасности предприятия как субъекта информационного права и информационных правоотношений. Основной целью данной статьи является изучение основных требований по обеспечению информационной безопасности предприятия.

В системе обеспечения безопасности все большее значение приобретает обеспечение информационной безопасности предприятия. Это связано с растущим объемом информации, с необходимостью ее хранения, передачи и обработки. Перевод значительной части информации в электронную форму, использование локальных и глобальных сетей создают качественно новые угрозы конфиденциальной информации.

Необходимо отметить, что в научной литературе отсутствует единый взгляд на содержание понятий «информационная безопасность» и «информационная безопасность предприятия». Так, В. Цымбалюк характеризует информационную безопасность в условиях формирования информационного общества как защиту информации в автоматизированных компьютерных системах, В. Фурашев считает, что информационная безопасность – это вид общественных информационных правоотношений по созданию, поддержке, охране и защите желательных для человека, общества

и государства безопасных условий жизнедеятельности, С. Гуцу предлагает рассматривать информационную безопасность как состояние защищенности потребностей в информации физических лиц, общества и государства, при котором обеспечивается безопасность их существования и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз. А. Литвиненко под информационной безопасностью понимает единство трех составляющих (обеспечение защиты информации, защиту и контроль национального информационного пространства, обеспечение надлежащего уровня информационной защиты). Интересным и одновременно дискуссионным является определение, в котором Б. Кормич отмечает, что информационная безопасность – это защита установленных законом правил, по которым осуществляются информационные процессы в государстве, обеспечивающие гарантированные Конституцией условия существования и развития человека, всего общества и государства. Л. Харченко, В. Липкан, А. Логинов определили, что информационная безопасность – это составляющая национальной безопасности, процесс управления угрозами и опасностями государственными и негосударственными учреждениями, отдельными гражданами, при котором обеспечивается информационный суверенитет Украины.

Таким образом, информационную безопасность следует рассматривать как обеспечение реализации национальных интересов с помощью разнообразных средств, имеющихся в ее распоряжении. Относительно понятия «информационная безопасность предприятия» необходимо отметить, что оно является чрезвычайно актуальным на современном этапе развития информационных технологий, который сопровождается введением информационных систем во все сферы деятельности человека. Так, А. Сороковская определяет информационную безопасность предприятия как общественные отношения по созданию и поддержанию на должном уровне жизнедеятельности информационной системы субъекта хозяйственной деятельности, М. Танцюра характеризует информационную безопасность предприятия как сохранение конфиденциальности, целостности и доступности информации (доступность – это свойство быть достижимым и пригодным к использованию в информационной среде; целостность – свойство защищенности точности и полноты данных; конфиденциальность – свойство защищенности информации от несанкционированного использования).

Учитывая данные определения, мы согласны с А. Марущаком, что информационная безопасность предприятия – это целенаправленная деятельность его органов и должностных лиц с использованием разрешенных методов и средств по достижению состояния защищенности информационной среды предприятия и обеспечению его нормального функционирования и динамичного развития.

Итак, суммируя вышесказанное, считаем необходимым подчеркнуть, что приоритетным направлением в процессе обеспечения информационной

безопасности предприятия является сохранение в тайне коммерчески важной информации, позволяющей успешно конкурировать на рынке товаров и услуг.

Опыт показывает, что для борьбы с правонарушениями в сфере обращения информации на предприятии необходима целенаправленная организация процесса защиты информационных ресурсов. Источник этого вида угроз может быть внутренним (собственные работники), внешним (например, конкуренты) и смешанным (заказчики – внешние, а исполнитель – работник фирмы). Как показывает практика, подавляющее большинство таких правонарушений осуществляются самими работниками предприятия.

Что же является непосредственным объектом правонарушений в сфере оборота информации? Прежде всего – это информация (данные). Правонарушитель получает доступ к информации, которая охраняется, без разрешения ее владельца или с нарушением установленного порядка доступа. Способы такого неправомерного доступа к компьютерной информации могут быть разными – кража носителя информации, нарушение средств защиты информации, использование чужого имени, изменение кода или адреса технического устройства, предоставление фиктивных документов на право доступа к информации, установка аппаратуры записи, подключаемой к каналам передачи данных. Причем доступ может быть осуществлен на территории предприятия, где хранятся носители, с компьютера на рабочем месте, с локальной сети, глобальной сети. Все угрозы объектам информационной безопасности по способу воздействия могут быть объединены в пять групп: информационные, физические, организационно-правовые, программно-математические, радиоэлектронные. Последствия совершенных противоправных действий могут быть различными:

- а) копирование информации (оригинал при этом сохраняется);
- б) изменение содержания информации по сравнению с той, которая была раньше;
- в) блокирование информации – невозможность ее использования при сохранении информации;
- г) уничтожение информации без возможности ее восстановления;
- д) нарушение работы компьютерной техники, системы или сети.

Проблемы, связанные с информационной безопасностью на предприятиях, могут быть решены только с помощью систематического и комплексного подхода. С методологической точки зрения, подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов. В обеспечении информационной безопасности нуждаются разные субъекты информационных отношений:

- государство в целом или отдельные его органы и организации;
- общественные или коммерческие организации (объединения), предприятия (юридические лица);
- отдельные граждане (физические лица).

Весь спектр интересов субъектов, связанных с использованием информации, можно разделить на такие категории: обеспечение доступности, целостности и конфиденциальности ресурсов информационной среды.

Иногда в ряд основных составляющих информационной безопасности включают защиту от несанкционированного копирования информации, но как нам видится, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясим понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это очевидно наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, принято выделять ее как важнейший элемент информационной безопасности.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий). Средства контроля динамической целостности применяются в частности при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. Но практическая реализация мер по обеспечению конфиденциальности современных информационных систем имеет в Украине серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми. Большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Значение каждой из составляющих информационной безопасности для разных категорий субъектов информационных отношений различно.

В случае государственных организаций во главу ставится конфиденциальность, поэтому скорее будет допущена возможность повреждения или уничтожения информации, чем ее разглашение. Также для государственных структур особую значимость имеет целостность информации. Доступность, как одна из составляющих информационной

безопасности, по отношению к двум другим составляющим имеет наименьшее значение.

Для коммерческих организаций ведущую роль играет доступность информации. Особенно ярко это проявляется в разных системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.). Примером может быть и поставщик интернет-услуг (бесплатный почтовый сервер). Обычно для такого учреждения очень важно обеспечить возможность постоянного доступа пользователей к сервису (скорость Интернета для пользователей так же важна).

Целостность – также важнейший аспект информационной безопасности коммерческих структур. Набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Если в качестве объекта выступает, например, значение суммы финансовых средств на счету клиента (остаток), то главная задача банка – обеспечить невозможность ее несанкционированного изменения (целостность). При этом в экстраординарных ситуациях можно пойти на временное отсутствие доступа к счету или разглашение данных. В то же время конфиденциальность в случае коммерческой информации играет заметно меньшую роль.

Целостность информации тесно связана с понятием надежности как технических, так и программных средств, реализующих процессы накопления, хранения и обработки информации. Из анализа угроз безопасности информации, целей и задач ее защиты следует, что достичь максимального (требуемого) уровня защищенности можно только за счет комплексного использования существующих методов и средств защиты. Комплексность является одним из принципов, которые должны быть положены в основу разработки, как концепции защиты информации, так и конкретных систем защиты. Цели защиты информации на объектах защиты могут быть достигнуты при проведении работ по таким направлениям:

- определение охраняемых сведений об объектах защиты;
- оценка возможностей и степени опасности технических средств разведки;
- выявление возможных технических каналов утечки информации;
- анализ возможностей и опасности несанкционированного доступа к информационным объектам;
- анализ опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты;
- разработка и реализация организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз;

- создание комплексной системы защиты;
- организация и проведение контроля состояния и эффективности системы защиты информации;
- обеспечение устойчивого управления процессом функционирования системы защиты информации.

Процесс комплексной защиты информации должен осуществляться непрерывно на всех этапах. Реализация непрерывного процесса защиты информации возможна только на основе систем концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлено только специалистами высокой квалификации в области защиты информации.

Для граждан на первое место можно поставить целостность и доступность информации, обладание которой необходимо для осуществления нормальной жизнедеятельности. Например, в случаях искажения информации во время выборов конфиденциальность не играет ключевой роли, хотя отметим, что физические лица сегодня являются самыми незащищенными субъектами информационных отношений.

Итак, на основании проведенного исследования можно отметить, что предприятия рассматриваются как субъекты информационного права, а потому мы должны изучать информационные правоотношения, в которые они практически вступают, реализуя полномочия, регулируемые нормами различных отраслей права.

При этом одним из важных аспектов, на котором должно быть сосредоточено внимание, является вопрос обеспечения информационной безопасности предприятия. Если процедуры создания, получения специальных статусов и разрешений, прекращения деятельности и надзора за такой деятельностью в большей степени относятся к предмету других отраслей права, то обеспечение информационной безопасности, потребность в котором, как автор пытался показать, проявляется в течение всего времени существования предприятия и его взаимодействия с другими субъектами, практически полностью относится к предмету информационного права. В то же время как невозможно в полной мере выделить информационную составляющую в деятельности предприятия, так очень сложно разграничить правовое регулирование этой сферы различными отраслями права.



«РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ» ЭЛЕКТРОННОЙ ПОЧТЫ GMAIL

Источник: блог Богдана-Флорина Поповичи
<https://bogdanpopovici2008.wordpress.com/2018/06/03/mecanismul-de-confidentialitate-gmail/>

Ещё один гвоздь в гроб архивного дела, который вбивает новый вызов архивистике. Сегодня мы протестировали новый «механизм обеспечения конфиденциальности» Gmail. Несколько лет тому назад Microsoft пробовал что-то подобное, но это не пошло (обычно после того, как электронное письмо загружено в Outlook, его трудно отозвать или удалить). Однако Gmail использует иной подход, при котором он сохраняет контроль над сообщением и, следовательно, имеет возможность эффективно блокировать доступ. Суть заключается в том, что адресату защищенного сообщения электронной почты доставляется ссылка на текст сообщения (примерно в том же духе, как сейчас проводятся фишинговые атаки), при переходе на которую Вы можете просмотреть содержимое письма в своём браузере. Всё построено на основе облачных технологий.

Последствия для управления документами и архивного дела:

1. Доступ к присланному по электронной почте сообщению может быть заблокирован: сегодня мы его видим, а завтра? Последствия оказываются разрушительными для систем документирования и архивов: Вы не только теряете контроль над полученной корреспонденцией, но Вы, возможно, даже не сможете получить к ней доступ. Я знаю, что это стандартная политика для секретной переписки, но это весьма проблематично с точки зрения обеспечения прозрачности государственного управления и деловой деятельности.

2. Захватывать сообщения электронной почты для возможного архивирования придётся в момент их получения. Это задача все равно будет проблематичной, поскольку отправитель может отключить возможности печати, пересылки и т.д. Я полагаю, что остается одна альтернатива – делать копию экрана; ничего себе получается штука!

3. Те, кто не подключен к интернету, но имеют доступ к электронной почте, ничего не смогут увидеть.

Комментарий: Впервые эта проблема появилась, наверное, лет десять тому назад, когда появилась возможность использовать инструменты управления правами доступа к электронному контенту в отношении офисных файлов – там тоже была возможность заблокировать доступ к файлу и фактически его уничтожить. Однако угроза так и не воплотилась в жизнь, наверное, потому, что, во-первых, с любителями подобных шуток отказывались иметь дело как государственные органы, так и представители бизнеса; во-вторых, в случае деловых споров суды с подозрением относились

к использованию сторонами подобных технологий; да и, в-третьих, это по большому счету скорее имитация защиты: никто не отменил ни фотоаппаратов и видеокамер, ни копий экрана, ни иных средств захвата информации. Посмотрим, что получится у Gmail.

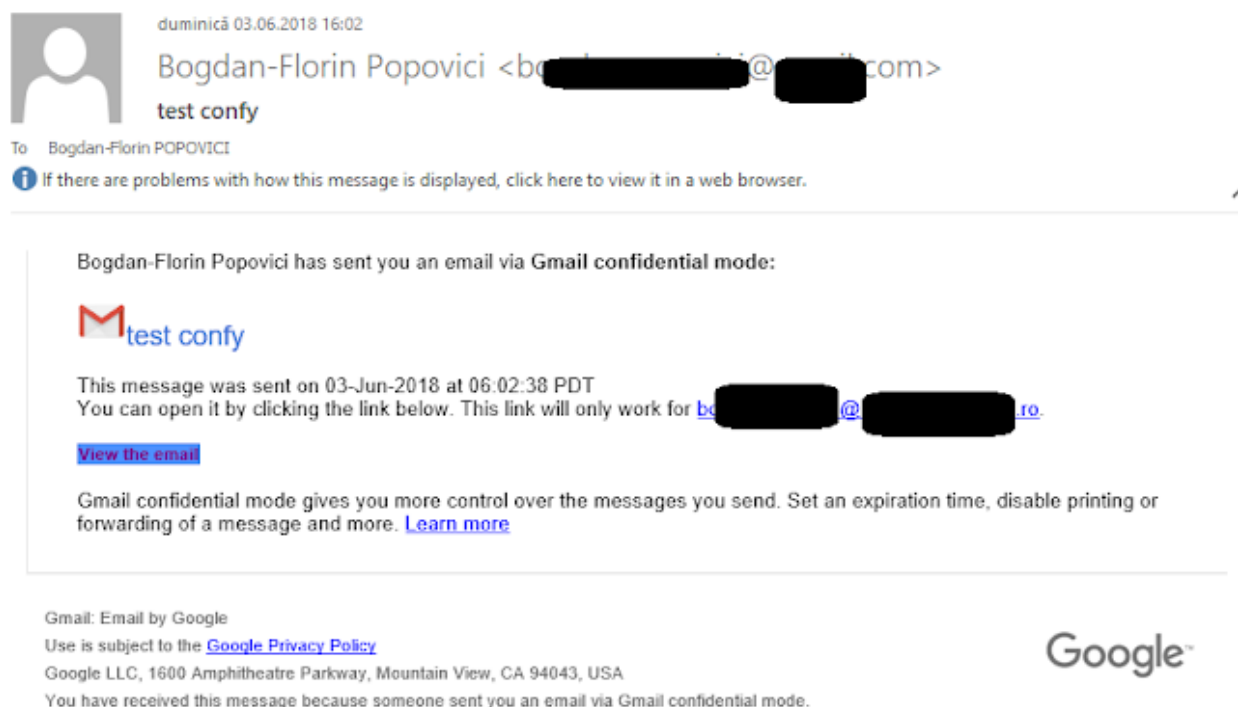


Рис. 1. Вот что видит получатель в почтовой системе – приглашение перейти по ссылке



ФРАНЦИЯ: ОПУБЛИКОВАН ПОРЯДОК ОКАЗАНИЯ УСЛУГ «ЭЛЕКТРОННОГО СЕЙФА»

Источник: Официальный правовой портал Франции
<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036964260&dateTexte=&categorieLien=id>
Автор: [Наташа Храмцовская](#)

На днях во Франции в «Официальном журнале Французской Республики» (Journal officiel de la République française, JORF, № 0123 от 31 мая 2018 года) был опубликован Декрет № 2018-418 от 30 мая 2018 года о порядке оказания услуг «электронного сейфа» (Décret № 2018-418 du 30 mai 2018 relatif aux modalités de mise en œuvre du service de coffre-fort numérique,

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036964260&dateTexte=&categorieLien=id>).

Услуги «электронного сейфа» – это одна из признаваемых законодательством возможностей хранения отдельными лицами и организациями своих электронных документов без ущерба для их правовой и доказательной силы (ещё одной возможностью является использование сертифицированных систем управления документами).

В Кодекс почтовых услуг и электронных коммуникаций (Code des postes et des communications électroniques), в его «Нормативную часть – Декреты Государственного Совета» (Partie réglementaire – Décrets en Conseil d'Etat), включена глава «Услуги «электронного сейфа»» (Service de coffre-fort numérique), содержащая один раздел «Оказание услуг электронного сейфа» (Mise en œuvre du service de coffre-fort numérique), состоящий из 6 статей.

Décret n° 2018-418 du 30 mai 2018 relatif aux modalités de mise en œuvre du service de coffre-fort numérique

[Masquer le panneau de navigation](#)

[Imprimer](#)

Navigation

Décret n°2018-418 du 30 mai 2018


▶ **Version initiale**

▶ [Version en vigueur au 4 juin 2018](#)

Version consolidée à la date du ...

Jour Mois Année

Ex: 2018



 [Sommaire](#)

 [Article 1](#)

JORF n°0123 du 31 mai 2018
texte n° 36

Décret n° 2018-418 du 30 mai 2018 relatif aux modalités de mise en œuvre du service de coffre-fort numérique

NOR: ECO1801826D

ELI: <https://www.legifrance.gouv.fr/eli/decret/2018/5/30/ECO1801826D/jo/texte>
Alias: <https://www.legifrance.gouv.fr/eli/decret/2018/5/30/2018-418/jo/texte>

Publics concernés : particuliers, professionnels, administrations.

Objet : modalités de mise en œuvre par l'Etat du service de coffre-fort numérique prévu par [l'article L. 103 du code des postes et des communications électroniques](#).

Ст. R.55-1. – Поставщик услуги «электронного сейфа» обязан предоставить четкую, справедливую и прозрачную информацию об условиях функционирования и использовании услуги до заключения контракта.

Перед тем, как пользователь будет связан договором об оказании услуги «электронного сейфа», поставщик услуг должен сообщить пользователю, читаемым и понятным образом, следующую информацию:

1. Тип предоставляемого пользователю пространства хранения и соответствующие условия его использования;
2. Применяемые технические механизмы;
3. Политика конфиденциальности;

4. Наличие и порядок осуществления гарантий хорошего функционирования;

5. Обязательство поставщика обеспечить соответствие услуги требованиям, установленным пп.1-5 статьи L103 (см. <https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000033207395&cidTexte=LEGITEXT000006070987&dateTexte=20180604>, это описание услуги «электронного сейфа», перевод которого можно найти здесь: https://rusrim.blogspot.com/2016/08/blog-post_4.html – Н.Х.).

Эта информация также должна быть доступной в Интернете и, при необходимости, обновляться.

Ст. R. 55-2. – Поставщик услуги «электронного сейфа» должен в технической документации указать, каким образом он обеспечивает соответствие требованиям, установленным в пп.1-5 статьи L.103, как это требуют положения данного раздела.

Ст. R. 55-3. – Целостность и доступность хранящихся в «электронном сейфе» данных и документов, а также точность сведений об их происхождения, обеспечиваются путем применения мер безопасности, которые отвечают текущему уровню техники.

Ст. R. 55-4. – Для обеспечения прослеживаемости операций, выполняемых с хранящимися в «электронном сейфе» данными и документами, а также доступности этих сведений пользователю, требуется принятие, по меньшей мере, следующих мер:

1. Регистрация и снабжение отметкой времени операций и попыток операций доступа;

2. Протоколирование операций, влияющих на содержимое или организацию данных и документов пользователя;

3. Протоколирование операций технического обслуживания, влияющих на данные и документы, хранящиеся в «электронных сейфах».

Сроки хранения этой контрольной информации в обязательном порядке должны быть упомянуты в контракте на предоставление услуг «электронного сейфа».

Ст. R. 55-5. – Идентификация пользователя при доступе к услуге «электронного сейфа» обеспечивается мерами и средствами электронной идентификации, адаптированным к требованиям по безопасности, предъявляемым к услуге.

Ст. R. 55-6. – Обеспечение, как это предусмотрено п.4 статьи L.103, исключительности доступа пользователя к его документам и данным или данным, связанных с использованием услуги, требует, по меньшей мере, принятия следующих мер:

1. Использование механизма управления доступом, позволяющего открывать «электронный сейф» только лицам, уполномоченным пользователем;

2. Применение мер безопасности для обеспечения конфиденциальности хранящихся документов и данных, а также соответствующих метаданных;

3. Шифрование услугой «электронного сейфа» всех документов и данных, хранящихся в электронном сейфе, а также перемещаемых в него или из него. Это шифрование должно выполняться с использованием криптографических механизмов, соответствующих текущему уровню технологий, и допускать изменение используемых алгоритмов и длин ключей. Соответствие текущему уровню технологий презюмируется в том случае, когда механизмы, применяемые в этих операциях шифрования, соответствуют правилам и рекомендациям Национального агентства по безопасности информационных систем (Agence nationale de sécurité des systèmes d'information) в отношении выбора криптографических механизмов и их параметров.



КОНФЕРЕНЦИЯ ИНФОДОКУМ-2018 «ЦИФРОВАЯ ЭКОНОМИКА»

Источник: YouTube / Google <https://www.youtube.com/watch?v=aoFFHJc9UvY>
https://docs.google.com/presentation/d/e/2PACX-1vQ2_zKCzL_kvqxaT6UfMJJaXQIgF3hXwCowsKPegh3H6oI5TlbqK7PIWAJN8Q_0dzBL8Q838JL0zcbkd/pub?start=false&loop=false&delayms=3000


6 – 7 июня 2018 года в Торгово-промышленной палате Российской Федерации состоялся профессиональный форум «Эффективный документооборот в эпоху цифровой экономики», организованный Гильдией управляющих документацией. В одном из докладов **«Цифровая экономика: модернизация законодательства в части управления документами»**, была дана оценка части тех законодательных инициатив, над которыми сейчас работают в рабочих группах, реализующих «дорожные карты». Можно сказать, что этот доклад стал продолжением выступления на конференции «Инфоархив-Власть 2017» в декабре 2017 года (см.: https://rusrim.blogspot.com/2017/12/2017_25.html).

Уже рассказывалось о том, что в Плане мероприятий по направлению «Нормативное регулирование» программы «Цифровая экономика Российской Федерации», который был утвержден Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (см.: https://rusrim.blogspot.com/2018/02/blog-post_0.html; это подраздел «Создание правовых условий для формирования сферы электронного гражданского оборота»), предусматривается внесение изменений в федеральные законы «Об архивном деле в Российской Федерации», «Об обязательном экземпляре документов», «Об информации, информационных технологиях и о защите

информации» и в иные нормативные правовые акты «в части уточнения понятия электронного документа, определения процедур хранения документов, в том числе электронных, использования и хранения электронного дубликата (электронного образа) документа». К сожалению, пока нельзя сказать о том, что в разработке законопроекта наметилось какое-то серьезное продвижение.

Еще одна тема, которая затронута в докладе – это электронный кадровый документооборот. По этому вопросу есть определенное движение вперед и, самое главное, уже понятно, в каком направлении будет меняться трудовое законодательство в ближайшее время.

Более подробную информацию смотри в источниках.



ИСО: ГОТОВИТСЯ СТАНДАРТ PDF/R ДЛЯ ХРАНЕНИЯ И ПЕРЕДАЧИ РАСТРОВЫХ ИЗОБРАЖЕНИЙ

Источники: сайт ИСО / сайт PDFRaster.org / YouTube
<https://www.iso.org/standard/75804.html>
http://www.pdfrafter.org/wp-content/uploads/2017/06/PDFrafter10_June-2017.pdf
<https://www.youtube.com/watch?v=-YeyOOm9ChM>



Как сообщает сайт Международной организации по стандартизации, начат процесс ускоренной подготовки и публикации **стандарта**

ISO/DIS 23504-1 «Приложения для управления контентом – Хранение и передача растровых изображений – Часть 1: Использование ISO 32000 (PDF/R-1)» (Document management applications - Raster image transport and storage - Part 1: Use of ISO 32000 (PDF/R-1)) объемом 15 страниц, см. <https://www.iso.org/standard/75804.html> и <https://www.iso.org/obp/ui/#!iso:std:75804:en> .

Разработкой стандарта занимается технический подкомитет ISO/TC171/SC2 «Документные файловые форматы, системы управления электронным контентом и аутентичность информации» (Document file formats, EDMS systems and authenticity of information), на основе документа, подготовленного некоммерческой организацией TWAIN Working Group.

В данный момент сведения о проекте можно найти на сайте <http://www.pdfrafter.org/>, принадлежащем организации-разработчику TWAIN Working Group.



В выложенной на сайте версии 1.0 спецификаций формата (см. http://www.pdfrafter.org/wp-content/uploads/2017/06/PDFrafter10_June-2017.pdf), в частности, отмечается следующее:

В настоящем документе описывается формат PDF/Raster – строгое подмножество файлового формата PDF для целей хранения, передачи и распространения многостраничных растровых изображений, в первую очередь отсканированных образов документов. PDF/Raster обеспечивает свойственную формату PDF многоплатформенность, и одновременно – ключевые функциональные возможности формата TIFF. Поддерживаются черно-белые, полутоновые и RGB-изображения. Варианты сжатия включают JPEG, CCITT Group 4 Fax без потерь, а также хранение несжатых графических образов.

Формат PDF/Raster была разработан благодаря сотрудничеству Рабочей группы по протоколу TWAIN, которая первой предложила концепцию этого

формата, и Ассоциации PDF (PDF Association), вкладом которой стал опыт и перспективы PDF-технологий, а также контакты с индустрией программного обеспечения, поддерживающего PDF, что позволило широкий спектр соответствующих точек зрения.

Формат PDF/Raster предназначен для использования в качестве стандартного формата хранения, передачи и распространения отсканированных документов. Как подмножество «полного» формата PDF, он опирается на существующую широкую поддержку просмотра, печати и обработки PDF-файлов. Поскольку он является очень узким подмножеством формата PDF, файлы в формате PDF/Raster гораздо проще создавать и интерпретировать, что позволяет ему заменять файловые форматы TIFF и JPEG при захвате и распространении результатов сканирования.

Формат PDF/Raster накладывает целый ряд ограничений на контент и структуру PDF-файлов, что дает следующие преимущества:

- Файлы могут быть прочитаны и записаны без использования полнофункционального PDF-анализатора или генератора;
- Обеспечивается эффективное создание PDF-файлов на основе растровых графических образов;
- Файлы могут создаваться с использованием буфера растровых данных фиксированного размера;
- При создании многостраничного файла необходимо дополнительно сохранить менее 1 килобайта данных на каждую страницу;
- Для поиска и извлечения изображений может быть использован сравнительно простой код;
- Файлы формата PDF/Raster могут быть быстро и легко идентифицированы как таковые программным обеспечением;
- Формат PDF/Raster поддерживает эффективные и легкодоступные алгоритмы сжатия.

Формат PDF/Raster имеет следующие важные преимущества перед полным PDF-форматом при хранении отсканированных документов:

- Есть возможность извлечь точные исходные растровые графические образы;
- Не требуется сложных программных средств для рендеринга;
- Создание файлов в таком формате является четко определенной задачей, что упрощает проектирование и тестирование.

Формат PDF/Raster имеет важные преимущества перед форматами TIFF и JPEG при хранении отсканированных документов:

- По сравнению с TIFF, у него гораздо меньше вариантов, и эти варианты проще;
- По сравнению с TIFF, алгоритмы сжатия проще, они лучше стандартизированы и лучше поддерживаются;
- По сравнению с TIFF, файлы PDF можно без дополнительных усилий просматривать и распечатывать на большем числе платформ платформ;

- В отличие от JPEG, формат PDF/Raster изначально является многостраничным и поддерживает хранение монохромных (черно-белых) изображений.

Дополнительная информация: На сайте YouTube выложена видеозапись 38-минутного доклада председателя Рабочей группы по протоколу TWAIN (TWAIN Working Group, <http://www.twain.org/> - некоммерческая организация, отвечающая за поддержку TWAIN) Джона Харью (Jon Harju), сделанного в мае 2017 года на конференции PDF Days Europe 2017 (<https://www.pdfa.org/final-agenda-of-the-pdf-europe-2017-available-as-download>), в котором он рассказывает о формате PDF/Raster, см. <https://www.youtube.com/watch?v=-YeyOOm9ChM>

В частности, Джон отметил, что формат PDF/R близок к формату PDF/A, и путем соблюдения ряда дополнительных ограничений можно обеспечить соответствие спецификациям PDF/A.



ШТАТ ВИКТОРИЯ, АВСТРАЛИЯ: ОНЛАЙН-РЕШЕНИЕ ORDA ДЛЯ РАЗРАБОТКИ И АКТУАЛИЗАЦИИ УКАЗАНИЙ ПО СРОКАМ ХРАНЕНИЯ И ДЕЙСТВИЯМ ПО ИХ ИСТЕЧЕНИИ

Источник: сайт PROV <https://prov.vic.gov.au/recordkeeping-government/learning-resources-tools/orda>

В электронную эпоху давно уже вышел из моды трудоёмкий и неэффективный бумажный процесс создания перечней документов с указанием сроков хранения, от которого наш Росархив пока не планирует оказываться (да и не сможет, учитывая отсутствие идей, денег и кадров). Первыми полностью перевели в электронную онлайн-среду межведомственное взаимодействие при разработке подобных нормативных документов американцы в рамках своей электронной архивной системы ERA. Сегодняшний пост посвящен аналогичному австралийскому решению ORDA – это перевод краткого описания этой системы, которое размещено на сайте Управления государственными документами австралийского штата Виктория (Public Record Office Victoria, PROV).

Онлайн-решение, поддерживающее разработку и актуализации указаний по срокам хранения и действиям по их истечении (Online Retention and Disposal Application, ORDA)

Что такое ORDA?

Решение ORDA - это веб-приложение, предназначенное для поддержки в онлайн-режиме разработки, представления на утверждение, публикации и последующей актуализации указаний по срокам хранения и действиям по их истечении (Retention and Disposal Authorities, RDA – *аналог наших Перечней*).

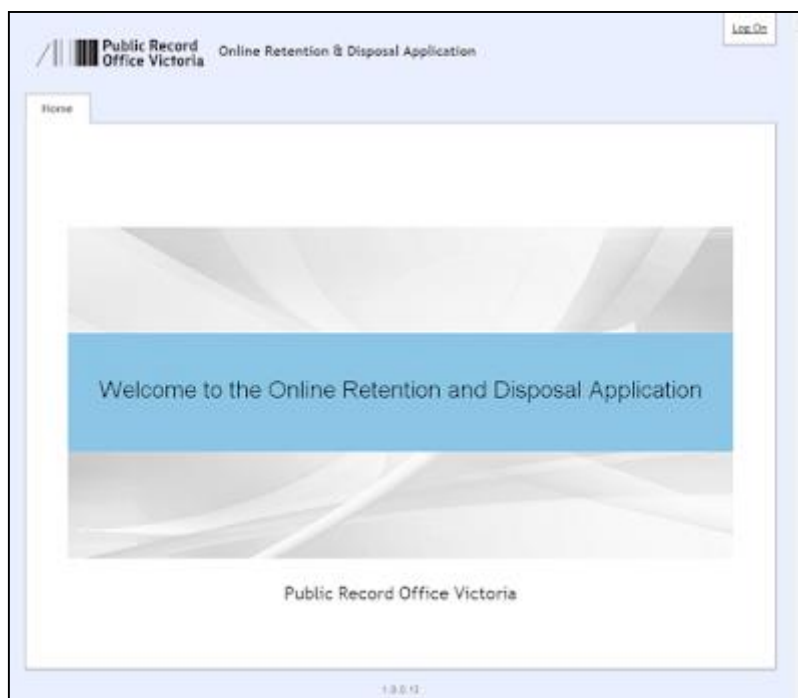
Приложение управляет полным комплексом соответствующих рабочих процессов, давая возможность Управлению государственных документов штата (Public Record Office Victoria, PROV), сотрудникам государственных органов и учреждений штата Виктория и привлеченным государственными органами поставщикам услуг совместно разрабатывать и выпускать указания по срокам хранения в онлайн-среде.

ORDA также поддерживает централизованную базу данных о сроках хранения и соответствующих решениях по итогам экспертизы ценности документов, в которой есть возможность поиска существующих прецедентов.

Вход в систему ORDA – на странице <http://orda.prov.vic.gov.au/> .

Кто может использовать ORDA?

Доступ к системе ORDA имеют сотрудники служб управления документами и информацией государственных органов, а также поставщики услуг, привлечённые государственными органами к разработке или пересмотру указаний по срокам хранения.



Стартовая страница системы ORDA

Как мне использовать ORDA?

Приложение ORDA доступно в Интернете. После начала официально одобренного проекта разработки указаний по срокам хранения сотрудники PROV выдадут Вам логин и пароль для входа в систему.

Сведения о том, как пользоваться ORDA, можно найти в руководствах по ORDA.



Мой комментарий: На той же странице выложены 8 руководств по ORDA:

- Руководство 1 «Вход в систему» (ORDA Guide 1 - Logging into ORDA),

https://www.prov.vic.gov.au/sites/default/files/files/media/orda_agency_g1_logging_on_to_orda_v1.1_final_ah_20180627.pdf

- Руководство 2 «Навигация в ORDA» (ORDA Guide 2 - Navigating in ORDA),

<https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-2-Navigating-in-ORDA.pdf>

- Руководство 3 «Доступ к Вашим указаниям по срокам хранения в ORDA» (ORDA Guide 3 - Accessing your RDA in ORDA),

<https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-3-Accessing-your-RDA-in-ORDA.pdf>

- Руководство 5 «Создание и редактирование условий и классов» (ORDA Guide 5 - Creating or editing terms and classes),

<https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-5-Creating-or-Editing-Terms-Classes.pdf>

- Руководство 6 «Действия по истечении сроков хранения, события-триггеры и обоснования» (ORDA Guide 6 - Disposal actions, triggers and justifications),

<https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-6-Disposal-Actions-Triggers-Justifications.pdf>

- Руководство 7 «Поиск указаний по срокам хранения» (ORDA Guide 7 - Searching RDAs),

<https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-7-Searching-RDAs.pdf>

- Руководство 9 «Поток рабочих процессов» (ORDA Guide 9 – Workflow),

<https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-9-Workflow.pdf>

- Руководство 10 «Отслеживание изменений и замечаний и предложений» (ORDA Guide 10 - Track changes and comments), <https://www.prov.vic.gov.au/sites/default/files/files/ORDA%20Guides/ORDA-Guide-10-Track-Changes-Comments.pdf>

Уверена, что подобную систему посылно создать и нам – ничего фантастического в ней нет. Ввод в эксплуатацию подобного решения позволил бы резко уменьшить трудозатраты, повысить качество перечней (в том числе за счет открытого и прозрачного публичного обсуждения), обеспечить их своевременную актуализацию и доступ заинтересованных сторон к актуальным версиям. Заодно ушли бы в небытие многочисленные бумажные документы, создаваемые сейчас в процессе разработки и утверждения перечней...



ИСО: ТЕХНИЧЕСКИЙ ОТЧЕТ ПО МИКРОКЛИМАТУ СРЕДЫ ХРАНЕНИЯ АРХИВНО-БИБЛИОТЕЧНЫХ МАТЕРИАЛОВ

Источник: сайт ИСО <https://www.iso.org/standard/66264.html>
<https://www.iso.org/obp/ui/#!iso:std:66264:en>



В июне 2018 года Международная организация по стандартизации (ИСО) опубликовала **технический отчет ISO/TR 19815:2018 «Информация и документация – Управление условиями окружающей среды при хранении архивных и библиотечных коллекций»** (Information and

documentation - Management of the environmental conditions for archive and library collections), объёмом 72 страницы, см. <https://www.iso.org/standard/66264.html> и <https://www.iso.org/obp/ui/#!iso:std:66264:en>.

В данном документе представлена информация о недавних обсуждениях и последних изменениях в рекомендациях и руководствах по управлению окружающей средой в области сохранения культурно-исторического наследия. Он включает результаты исследований в области консервации по предупредительным мерам и по пассивному контролю, обеспечиваемому специальными методами строительства и реконструкции; достижения в области технологий управления окружающей средой; а также вопросы энергоэффективности и влияния изменения климата.

Данный документ адресован архивам, библиотекам и другим учреждениям, располагающим объёмными коллекциями материалов на бумажных носителях. В архивах и библиотеках также имеются коллекции, включающие материалы, зафиксированные на плёнке, магнитных носителях, на коже и других органических, неорганических и составных носителях. Перед этими учреждениями стоит уникальная задача продления срока службы этих материалов для целей доступа и использования их настоящими и будущими поколениями. Параметры окружающей среды играют ключевую роль в продлении срока службы всех этих материалов.

Настоящий документ предназначен для использования при планировании деятельности по обеспечению долговременной сохранности, а также текущего управления параметрами среды постоянного хранения архивных и библиотечных коллекций, и применим в отношении любых коллекций, постоянно хранящихся в учреждении.

Содержание документа следующее:

Предисловие

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Общие положения
5. Управление окружающей средой в целях оптимизации живучести и долговременной сохранности
6. Температура
7. Относительная влажность
8. Климат и его последствия для коллекций
9. Насекомые и другие вредители
10. Загрязнения окружающей среды
11. Свет
12. Установление требований к температуре и относительной влажности
13. Измерение влажности (гигрометрия)

14. Хорошие практики обеспечения стабильности и живучести

15. Инструменты для обучения и оценки

Приложение А: Экономное энергопотребления

Приложение В: Воздействие температуры

Приложение С: Воздействие относительной влажности

Приложение D: Материальный ущерб, связанные с воздействием температуры и относительной влажности

Приложение E: Источники загрязнений и их воздействие на материалы, существенное для архивных и библиотечных коллекций

Приложение F: Комбинированное воздействие температуры, относительной влажности, света и загрязнений

Библиография



КОНСОРЦИУМ ВСЕМИРНОЙ ПАУТИНЫ W3C ВЫЛОЖИЛ ПРОЕКТ ПЕРЕСМОТРЕННОЙ ВЕРСИИ ПУБЛИКАЦИИ «НЕДОСТАТКИ САРТСНА В ПЛАНЕ ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ»

Источник: сайт консорциума W3C

<https://www.w3.org/blog/news/archives/7143>

<https://www.w3.org/TR/2018/WD-turingtest-20180703/>

Данная заметка была опубликована на сайте Консорциума Всемирной паутины W3C (The World Wide Web Consortium (международного сообщества, разрабатывающего открытые стандарты, обеспечивающие развитие интернета в долговременной перспективе)).

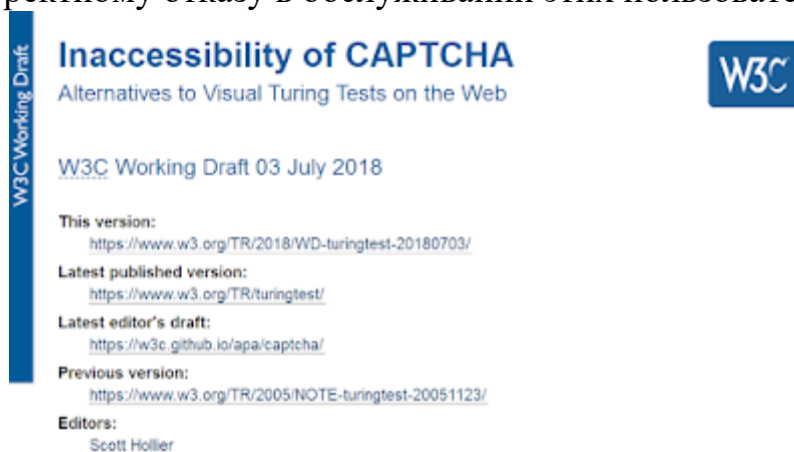
Рабочая группа по способствующей доступности архитектуре платформ (Accessible Platform Architectures Working Group) опубликовала рабочий проект пересмотренной версии публикации «**Недостатки САРТСНА в плане обеспечения доступности. Альтернативы визуальному тесту Тьюринга в интернете**» (Inaccessibility of САРТСНА - Alternatives to Visual Turing Tests on the Web), см. <https://www.w3.org/TR/2018/WD-turingtest-20180703/>.

Для справки: Капча (от САРТСНА — англ. Completely Automated Public Turing test to tell Computers and Humans Apart — полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) — компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером. Термин появился в 2000 году. Основная идея теста: предложить пользователю такую

задачу, которая с лёгкостью решается человеком, но крайне сложна и трудоёмка для компьютера. (Википедия, см. <https://ru.wikipedia.org/wiki/Капча>)

Со времени выхода в свет последней редакции этого документа возможности роботов по преодолению теста CAPTCHA выросли, и в то же время появились новые технологии для аутентификации пользователей-людей. Данная обновленная редакция приводит документ в соответствие с этими новыми реалиями.

За прошедшие годы для различения пользователей веб-сайтов – людей от роботов применялись различные подходы. Хотя традиционный метод CAPTCHA, предлагающий пользователю идентифицировать спрятанный в изображении текст остается всеобщепотребительным, все большую известность приобретают альтернативные механизмы. От пользователей обычно требуется выполнить задачу, которая, как считается, посильна для людей и сложна для роботов,- но сам характер задачи по своей природе исключает многих людей с ограниченными возможностями, что приводит к некорректному отказу в обслуживании этих пользователей.



The image shows a screenshot of a W3C Working Draft document. On the left, there is a vertical blue bar with the text 'W3C Working Draft' written vertically. The main content area has a white background with blue text. The title is 'Inaccessibility of CAPTCHA' in a large blue font, followed by the subtitle 'Alternatives to Visual Turing Tests on the Web' in a smaller blue font. To the right of the subtitle is the W3C logo, which consists of the letters 'W3C' in white on a blue square background. Below the title and subtitle, the text reads 'W3C Working Draft 03 July 2018'. Further down, there are several lines of text providing version information: 'This version:' followed by a URL, 'Latest published version:' followed by a URL, 'Latest editor's draft:' followed by a URL, and 'Previous version:' followed by a URL. At the bottom, it says 'Editors:' followed by the name 'Scott Hollier'.

Комментарий: Я сама не раз сталкивалась даже на российских веб-сайтах с такими вариантами капча, которые без приличного знания английского и других иностранных языков решить проблематично, не говоря уже об умении углядеть текст в мешанине графических элементов. Конечно, чаще всего такие сложные шарады – результат наплевательского отношения сисадмина :(Результаты исследований также показывают, что многие популярные варианты CAPTCHA уже не являются особенно эффективными или безопасными, поэтому необходимо рассмотреть альтернативные подходы к блокированию ботов, обеспечивая при этом возможность прохождения этих тестов людьми с ограниченными возможностями. В настоящем документе рассматривается ряд потенциальных решений, которые позволяют системам идентифицировать пользователей-людей, а также то, в какой мере эти решения адекватны для людей с ограниченными возможностями.

История эволюции методов CAPTCHA показала, что традиционные решения, такие, как спрятанные в изображениях текстовые символы, не

только сложны для людей с ограниченными возможностями, но и небезопасны. В то время, как большинство используемых CAPTCHA-методов по-прежнему создают проблемы для людей с ограниченными возможностями, недавно появившиеся методы, в том числе reCAPTCHA от Google, аутентификация с использованием нескольких устройств и распространение систем с единой точкой идентификации (Federated identity systems) в настоящее время предлагают наиболее доступные и гибкие варианты при отделении людей от роботов.

Хотя некоторые решения CAPTCHA лучше других, в настоящее время нет «идеального» решения. Важно поэтому проявлять осторожность с тем, чтобы любая реализованная технология CAPTCHA правильно идентифицировала людей с ограниченными возможностями как людей.



ФОНД «ОТКРЫТАЯ СОХРАННОСТЬ» ОПУБЛИКОВАЛ СВОЮ НОВУЮ СТРАТЕГИЮ НА 2018 – 2021 ГОДЫ

Источник: Сайт Фонда «Открытая сохранность» («Открытые планеты») / блог Бекки Макгиннес <http://openpreservation.org/news/open-preservation-foundation-launches-new-strategy/>

Автор: Наташа Храмцовская

Фонд «Открытая сохранность» (Open Preservation Foundation, OPF) опубликовал 4 июля 2018 года свою новую стратегию, изложив в ней долгосрочные направления деятельности организации.



Стратегия определяет место OPF в ландшафте электронной сохранности и выбор тех задач, инструментов и проектов, на которые Фонд обратит внимание.

Новые базовые ценности отражают фундаментальные убеждения Фонда и определяют поведение организации. Основное внимание в Стратегии уделяется разработке базового инструментария OPF (OPF reference toolset) и дорожных карт для инструментов на основе открытого исходного кода, используемых для обеспечения долговременной сохранности, которые OPF курирует. В Стратегии названы мероприятия, направленные на совершенствование передовой практики и программы обмена знаниями Фонда.

Барбара Сирман (Barbara Sierman), председатель совета директоров OPF и консультант по вопросам электронной сохранности Национальной библиотеки Голландии, так прокомментировала это событие:

«Наша новая стратегия объединяет все направления деятельности Фонда в один чёткий план, предусматривающий практические действия, а также устанавливает метрики для оценки его эффективности. Мы хотели бы поблагодарить наших членов за их вклад, который помог обеспечить соответствие Стратегии их потребностям и приоритетам».

Исполнительный директор Фонда «Открытая сохранность» Мартин Ригли (Martin Wrigley) в свою очередь отметил:

«Мы рады опубликовать новую стратегию, которая представляет наши планы на будущее. Мы обновили наше видение и миссию, и призываем все организации, которые разделяют наши цели, присоединиться к нам с тем, чтобы способствовать успешности стратегии».

Документ объёмом 12 страниц доступен по адресу http://openpreservation.org/documents/public/OPF_Strategy_2018.pdf

Бекки Макгиннес (Becky McGuinness)

Мой комментарий: Свою миссию Фонд определил следующим образом:

«Способствуя коллективно используемым решениям задачи эффективного и продуктивного обеспечения долговременной сохранности электронных материалов, Фонд «Открытая сохранность» является лидером совместных усилий по созданию, поддержанию и развитию базового набора стабильных инструментов для электронной сохранности на основе открытого исходного кода и вспомогательных ресурсов.

Этот набор инструментов (включающий программное обеспечение и стандарты) позволяет организациям оценивать, проверять, документировать, смягчать риски и обрабатывать подлежащий сохранению электронный контент в соответствии с желаемыми политиками и наилучшей практикой сообщества».

В числе основных ценностей OPF названы следующие:

- Открытость;
- Деятельность в соответствии с нуждами организаций-членов;

- Стремление к сотрудничеству и инклюзивности (недискриминационности);
- Инновационность.



ХОРВАТИЯ: ПРИНЯТ НОВЫЙ ЗАКОН ОБ АРХИВНЫХ МАТЕРИАЛАХ И АРХИВАХ

Источник: сайт парламента Хорватии
<http://www.sabor.hr/konacni-prijedlog-zakona-o-arhivskom-gradivu-i-arh>
<https://had-info.hr/arhivistika-u-hrvatskoj/162-usvojen-novi-zakon-o-arhivskom-gradivu-i-arhivima>

Хорватский парламент на своей восьмой сессии, проведенной 29 июня 2018 года, 72 голосами «за» при 20 «против» и 15 воздержавшихся принял **новый «Закон об архивных материалах и архивах»** (Zakon o arhivskom gradivu i arhivima). Закон вскоре будет опубликован в «Официальном вестнике» (Narodne novine) и вступит в силу.



По мнению известного хорватского специалиста Хрвое Станчича (см. <https://www.facebook.com/hrvoje.stancic/posts/10216767844811503>), «теперь появится возможность оцифровывать бумажные документы, уничтожать – после получения соответствующего разрешения – бумажные оригиналы и использовать оцифрованную версию на правах оригинала».

В числе 5 основных целей закона (ст.2) явным образом названо «обеспечение, создания, сохранения и конвертации документальных и архивных материалов в цифровую форму».

В статье 3 даны следующие определения:

d) Документальные материалы [по-нашему, документы] в цифровой форме – это материалы в цифровой форме, записанные и хранимые на машиночитаемом носителе информации, которые были изначально созданы таким виде либо были получены путем преобразования материалов в цифровую форму.

е) Документальные материалы в цифровой форме постоянного хранения - это материалы, контент которых записан в цифровой форме и хранится на машиночитаемом носителе информации, при этом такая цифровая форма (формат) и носитель информации обеспечивают эффективное постоянное хранение и соответствие уровню развития технологий, в соответствии с настоящим Законом.

В статье 6 «Обязанности по систематическому управлению документальными материалами» в числе обязанностей государственного органа названы (п.1):

- Установление правил и процедур создания государственных документов в цифровой форме;
- Обеспечить преобразование архивных материалов в физической или аналоговой форме в цифровую форму.

В статье 8 «Преобразование материалов в цифровую форму» сказано следующее:

(1) Документарные материалы могут быть преобразованы в цифровую форму с целью обеспечения их защиты, доступности и для других целей, в соответствии с правилами, упомянутым в пункте 2 статьи 6 настоящего Закона (*речь идёт о подзаконном нормативном акте, определяющем условия и способы создания, сохранения, обработки, оценки, преобразования в цифровую форму, извлечения и раскрытия документальных материалов; а также способ проверки профессиональной квалификации в сфере управления документальными материалами, находящимися вне архивов, который должен быть утверждён министром культуры*).

(2) Упомянутое в п.1 преобразование материалов производится способом, обеспечивающим надежность и удобство использования материалов в соответствии с положениями настоящего Закона:

- Должны быть сохранены все существенные свойства, компоненты, эффекты и удобство использования исходного материала (сохранение целостности материала);
- Преобразование материала осуществляется таким образом, чтобы обеспечить разумную уверенность в отсутствии каких-либо несанкционированных и недокументированных добавлений, изменений или удаления свойств материалов;
- Процесс преобразования должен быть выполнен в соответствии с установленными правилами и надлежащим образом задокументирован с целью обеспечения и проверки правильности и качества преобразования;
- Преобразование материалов, защищаемых авторским правом, осуществляется в соответствии с положениями законодательства об авторском праве;
- Процесс преобразования должен быть осуществлен в соответствии с другими нормами, регламентирующими условия и процедуры преобразования определенных типов документальных материалов.

(3) Документальной является форма, в которую материалы преобразованы в точном соответствии с оригиналами, если преобразование в иную форму осуществлено в соответствии с положениями пункта 2 настоящей статьи и правилами, упомянутым в пункте 2 статьи 6 настоящего Закона.

(4) Способ преобразования материала в другую форму, характеристики технологии и процедуры, обеспечивающие разумную уверенность в отсутствии каких-либо несанкционированных и недокументированных добавлений, изменений или удаления свойств материалов или конкретных данных и в исполнении других требований по сохранению удобства использования документальных материалов, регулируется правилами, упомянутым в пункте 2 статьи 6 настоящего Закона.

Согласно п.1 ст.9, «Государственные органы должны обеспечить, чтобы государственные документальные материалы, созданные в результате его деятельности, были в форме, пригодной для использования и надежного преобразования в цифровую форму для их сохранения, передачи на архивное хранение и повторного использования».

В статье 12 «Отбор и уничтожение государственных документальных материалов», в частности, сказано:

(1) Публичные документальные материалы в физической форме, сроки хранения которых истекли и которые более не имеют значения для текущей деятельности их создателя, а также не имеют архивной или культурной ценности в соответствии с положениями настоящего Закона, могут быть выделены и уничтожены.

(2) Публичные документальные материалы, упомянутые в пункте 1 настоящей статьи, которые были преобразованы в цифровую форму в соответствии с настоящим Законом, могут быть отобраны и уничтожены даже до истечения срока хранения, если иное не предусмотрено настоящим Законом или другим нормативно-правовым актом.



ЕВРОСОЮЗ: ОПУБЛИКОВАНЫ НОВЫЕ СТАНДАРТЫ СЕМЕЙСТВА LOTAR

Источник: сайт Британского института стандартов
<https://shop.bsigroup.com/>

Автор: Наташа Храмцовская

Я уже рассказывала (см. <https://rusrim.blogspot.com/2015/01/1.html>) о деятельности организации LOTAR International (<http://www.lotar-international.org/>), целью которой является разработка, тестирование,

публикация и поддержка стандартов долговременной архивации таких электронных цифровых данных, как 3D-модели, данные САПР и PDM-систем (от Product Data Management, PDM – управление данными об изделии). Эти стандарты должны специфицировать проверяемые процессы архивации и извлечения.

Для нас эти стандарты также представляют интерес, поскольку быстро растёт внимание как к тематике электронных архивов, так и к проблеме обеспечения долговременной сохранности электронной научно-технической и опытно-конструкторской документации.

В 2018 году в рамках работы над стандартом **EN 9300 «Обеспечение долговременной сохранности и возможности использования электронной документации на технические продукты, такой, как 3D-модели, данные САПР и PDM-систем, в аэрокосмической отрасли»** (Long Term Archiving and Retrieval of digital technical product documentation such as 3D, CAD and PDM data within the aerospace industry, LOTAR) были опубликованы следующие документы:

- **Часть 2 «Требования»** (Requirements), см. <https://shop.bsigroup.com/ProductDetail?pid=000000000030185698>

- В данном стандарте рассматриваются требования к долговременной архивации электронной информации об изделиях, применимые к международной аэрокосмической промышленности. Данные должны быть доступны во исполнение нормативно-правовых, договорных и деловых требований.

- В начале данного документа перечисляются основные деловые требования в отношении долговременной архивации электронных данных об изделиях. Хотя эти требования сами по себе не являются нормативными, однако, когда решается задача обеспечения доступности данных в течение длительного периода времени, фундаментальным принципом является одновременное обеспечение доступности сведений о контексте деловой деятельности, необходимых для интерпретации данных.

- В данном стандарте используется эталонная модель OAIS для обеспечения сопоставимости с другими подходами к обеспечению сохранности информации. Однако OAIS является стандартной эталонной моделью для сравнения, а не стандартом для реализации. Соответственно, настоящий документ определяет требования к процессам (и взаимосвязанным технологиям), которые должны обеспечить доступность данных в течение срока службы изделия, и делает это в терминах модели OAIS.

- Стандарт также рассматривает вопросы управления эволюцией технологий, которое необходимо для обеспечения доступности данных и их пригодности к использованию в течение требуемого периода хранения.

- **Часть 10 «Обзор потоков данных»** (Overview Data Flow) , см. <https://shop.bsigroup.com/ProductDetail/?pid=000000000030139216>

- В данной части содержится общее описание рекомендованных процессов архивации 3D-данных о продуктах, например пространственных данных из CAD и PDM-систем. Более подробно эти процессы описаны в частях с 11 по 16.

- **Часть 200 «Общий подход к долговременной архивации и извлечению информации о структуре продукта»** (Common concepts for Long term archiving and retrieval of product structure information), см. <https://shop.bsigroup.com/ProductDetail?pid=000000000030329131>

- Данная часть охватывает долговременную архивацию (LTA and R) данных об управлении продуктом и соответствующей информацией о взаимосвязанных процессах (например, требования к структуре продукта). Что касается информации, относящейся к процессам, то в документе рассматриваются только результаты процессов, поскольку они имеют стабильные и статические характеристики. Не рассматривается workflow-процесс, используемый для создания информации. Документ охватывает итоговую информацию, такую, как авторизующие изменения документы, утверждения / подписи, САПР-модели, данных об атрибутах.



НОВАЯ ЭРА СОТРУДНИЧЕСТВА В ПРОВЕДЕНИИ ИССЛЕДОВАНИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЭЛЕКТРОННЫХ МАТЕРИАЛОВ

Источник: блог Коалиции по электронной сохранности (Digital Preservation Coalition, DPC) <https://dpconline.org/blog/a-new-era-in-collaboration-in-digital-preservation-research>

Автор: Джон Тилбери директор по технологиям компании Preservica

Вы, возможно, уже видели выпущенное на этой неделе объявление (см. <https://preservica.com/resources/press-releases/arkivum-artefactual-the-open-preservation-foundation-and-preservica-collaborate-on-new-jisc-initiative-for-sharing-preservation-action-best-practice> - *для доступа может потребоваться анонимайзер*) о финансируемом британским Объединенным комитетом по информационным системам (Joint Information Systems Committee, JISC, <https://www.jisc.ac.uk/>) совместном проекте, который должен объединить усилия в области исследований компаний Arkivum (<https://arkivum.com/>), Archivemata (<https://www.archivemata.org/en/>), Preservica (<https://preservica.com/>) и Фонда «Открытая сохранность» (Open Preservation Foundation, OPF, <http://openpreservation.org/> - ранее известный как фонд «Открытые планеты», *Open Planets Foundation*), с тем, чтобы организовать обмен информацией об опыте обеспечения долговременной сохранности электронных данных.

Я, как член этой новой команды, буду рад поделиться своими мыслями о том, как всё это произошло и к чему это может привести. Данное событие может стать началом новой эры совместных исследований, проводимых всеми новаторами в области электронной сохранности, и в результате могут быть получены два очень важных результата – электронная сохранность может стать лучше, и обеспечивать её может стать проще.

Я проработал 20 лет в сфере электронной сохранности, и меня очень огорчает то, что многие «острова» передового опыта и практики изолированы друг от друга и сведения о них распространяются только через локальные группы, на конференциях и в определенных сообществах пользователей конкретных продуктов. Многие не известны за пределами разработавших их организаций и учреждений, несмотря на вложенные в них творческие усилия и детальные исследования. Это иронично, поскольку наше сообщество в основном неконкурентное и его члены с удовольствием учатся друг у друга – но у них нет для этого эффективного механизма. В ряде своих докладов на конференции Специальной тематической группы по вопросам обеспечения сохранности и архивации (Preservation and Archiving Special Interest Group, PASIG, <http://sun-pasig.ning.com/>) я настоятельно призывал к более тесному сотрудничеству между всеми игроками в этой области.

Именно такого рода проблемы призван решить недавно объявленный проект создания **реестра мер по обеспечению долговременной сохранности** (Preservation Actions Registry, PAR). Эта амбициозная инициатива финансируется Джоном Кэй (John Kaye) из JISC как часть проекта Общих услуг по работе с научно-исследовательскими данными (Research Data Shared Service, RDSS, <https://www.jisc.ac.uk/rd/projects/research-data-shared-service>) с целью дать пользователям системы наилучшие рекомендации о том, как им обеспечить долговременную сохранность тех научных данных, за сохранение которых они несут ответственность. Реестр позволит пользователям сосредоточить свои усилия на исследованиях, а не на вопросах электронной сохранности, будучи уверенными в том, что их контент будет доступен в будущем. Поскольку RDSS включает в себя как решение Preservica, так и решение Archivemata, необходимо, чтобы эти системы могли делиться друг с другом передовой практикой с тем, чтобы пользователи могли учиться у всех, а не только у тех, кто пользуется такой же системой.

Партнеры RDSS по обеспечению электронной сохранности, - Arkivum, Archivemata, а также наша компания Preservica, - очень позитивно отнеслись к данной инициативе. На самом деле в прошлом было сделано немало попыток реализовать подобную концепцию, главным образом, путем создания супер-реестров, в названии которых присутствовали слова «окончательный» или «глобальный». Однако на этот раз проект является более реалистичным и нацелен на конкретный вариант использования, и все партнеры быстро согласились его поддержать; а затем к этой инициативе присоединился Фонда «Открытая сохранность» (OPF), который будет

представлять точку зрения более широкого сообщества и имеет возможность размещать в будущем любых общие реестры.

Команда проекта

Команда проекта в совокупности обладает колоссальным опытом, и её возглавляют следующие эксперты:

- от Arkivum - Мэтью Аддис (Matthew Addis);
- от Archivemata - Джастин Симпсон (Justin Simpson);
- от OPF - Карл Уилсон (Carl Wilson);
- от Preservica - Джек О'Салливан (Jack O'Sullivan);
- от JISC – Пол Стоукс (Paul Stokes).

План заключается в том, что, как только будет готова демонстрирующая работоспособность подхода пилотная версия (Proof of Concept), протоколы и модель данных будут свободно доступны для всех пользователей по всему миру, и мы будем приветствовать присоединение к проекту многих новых участников.

Обмен знаниями в рамках RDSS

Как я уже сказал выше, первоначальные усилия будут направлены на удовлетворение потребностей британских вузов, участвующих в проекте JISC RDSS - Общих услуг по работе с научно-исследовательскими данными. Исследователи получают возможность получать актуальные рекомендации по обеспечению электронной сохранности и действовать в соответствии с ними, что повысит ценность RDSS для академического сообщества Великобритании.

Идея проекта заключается в совместной работе над механизмами обмена и распространения используемых в различных системах наилучших практик выполнения действий по обеспечению долговременной сохранности. Основное внимание при этом будет уделено протоколам обмена, общей модели данных и развертыванию API-интерфейсов для чтения и подготовки рекомендаций. Под «действиями по обеспечению долговременной сохранности» (Preservation Actions) мы понимаем методы идентификации файловых форматов, извлечения свойств / метаданных из файлов, списки свойств / метаданных, которые можно извлечь (и что они означают), методы проверки файлов, миграции файлов из одного формата в другой и способы их отображения. Пользователи решений Preservica и Archivemata смогут делиться своими правилами и видеть, какие правила используют их коллеги - и применять их в своих системах.

В рамках данного проекта будет протестирована концепция такого обмена на основе общей модели данных и опубликованных API-интерфейсов. Эта часть работы завершится в конце июля, и ряд дальнейших работ запланирован на следующие несколько месяцев.

Обмен знаниями со всем сообществом

Подтверждение работоспособности концепции - это только начало. В ходе дальнейшей работы будут расширены и сделаны более продуктивными интерфейсами; это поощрит большее число пользователей присоединиться к

этой инициативе. В их числе будут выполняющие научно-исследовательскую работу практики и отраслевые эксперты, имеющие детальные знания о конкретных типах контента - например, об аудиовизуальных материалах, PDF-документах или научно-технической и опытно-конструкторской документации. Любой, кого интересует передовой опыт, сможет одним щелчком мыши получить совет от ведущих специалистов мира.

Существует также возможность немедленной публикации наилучшей практики в действующих системах, что позволит пользователям, желающим «принять значения по умолчанию» доверять центральному органу, распространяющему готовую для широкого применения, проверенную передовую практику, без необходимости обновления систем. Эта возможность представляется мне наиболее интересной, поскольку она дает возможность пользователям с небольшим опытом в области электронных технологий эффективно использовать сложные, порой даже пугающе сложные технологии электронной сохранности.

Дополнительная информация

Более подробную информацию о проекте можно найти здесь: www.parc core.org (или <https://parcore.readme.io/>). Мы также представим совместный доклад и статью о проекте PAR на конференции iPres, которая пройдет в этом году в Бостоне 24-27 сентября 2018 года. Полный текст статьи, которая называется «Обеспечение интероперабельности в электронной сохранности посредством использования реестров мер по обеспечению долговременной сохранности» (Digital Preservation Interoperability through Preservation Actions Registries), доступен по адресу <https://ndownloader.figshare.com/files/12127601>.

Совместная работа

С моей точки зрения, замечательно, что конкуренты могут работать вместе с тем, чтобы помочь создать механизмы для решения существующих проблем электронной сохранности. Эти проблемы не по силам одной отдельной компании, и в результате такого сотрудничества в выигрыше будут пользователи как решения Archivemata, так и решения Preservica. Я надеюсь, что в будущем мы будем вспоминать сегодняшние события как поворотный момент в обмене информацией об обеспечении электронной сохранности, способствовавший быстрому ускорению исследований, сокращению дублирования усилий и получению всеми, кто в этом нуждается, наилучших советов, как только те будут опубликованы.



НАЦИОНАЛЬНЫЕ АРХИВЫ ВЕЛИКОБРИТАНИИ ТЕСТИРУЮТ ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙНА ДЛЯ ЦЕЛЕЙ ОБЕСПЕЧЕНИЯ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ИСТОРИЧЕСКИХ ДОКУМЕНТОВ

Источник: сайт ETHNews.com <https://www.ethnews.com/uk-national-archives-tests-using-blockchain-for-historical-document-preservation>

Автор: Тим Прентис

В Великобритании в рамках совместного научно-исследовательского проекта изучаются возможности для использования технологии блокчейна для обеспечения точности исторических документов.

Девять месяцев назад в Университете Суррея (University of Surrey) в сотрудничестве с Институтом открытых данных (Open Data Institute) и Национальными Архивами Великобритании началась работа над исследовательским проектом на основе блокчейн-технологий ARCHANGEL (*Этот проект представлен в недавно опубликованной статье «ARCHANGEL – Доверенные архивы электронных государственных документов» (ARCHANGEL: Trusted Archives of Digital Public Documents), см. <https://arxiv.org/pdf/1804.08342.pdf>*). Этот проект, финансируемый Исследовательскими советами Великобритании (Research Councils UK), представляет собой попытку использовать технологию блокчейна для того, чтобы сделать невозможным внесение несанкционированных изменений в исторические документы.

Проект, который первоначально планировался на 18 месяцев, теперь, как ожидается, продлится два года.

Хеши контента электронных документов могут быть размещены в блокчейне, где изменения можно контролировать (*зафиксированные в блокчейне данные модифицировать невозможно, поэтому, сравнивая сохраненный в блокчейне хеш с текущим значением хеша, можно контролировать целостность электронного документа*). Хотя этот подход и не решает проблему фальсификации исходных документов, он позволит убедиться в том, что документ не был изменён в тот период, когда он находился под контролем самого архива, начиная с момента, когда хеш документа был записан в блокчейн. «Нас особенно интересуют те ситуации, когда архив хранит информацию, которая в настоящее время закрыта [для широкой общественности]. Хеши мы записываем в блокчейн сегодня. А впоследствии ... когда информация может быть раскрыта, люди смогут проверить - когда увидят раскрытую информацию, - что за период архивного хранения она не была изменена», - сказал в недавнем интервью

информационному агентству EThNews директор Национальных Архивов по электронным сервисам (Digital Director) Джон Шеридан (John Sheridan).

Организации-участники проекта сейчас решают вопрос о том, следует ли создавать ARCHANGEL как блокчейн с ограниченным доступом (permissioned blockchain), что будет означать, что только участвующие в проекте национальные архивы, университеты и библиотеки смогут записывать информацию, при этом информация в блокчейне будет свободно доступна на чтение.

Шеридан объяснил, что такой подход позволит избежать главной проблемы публичных блокчейнов: «Мы полагаем, что одним из преимуществ блокчейна с ограниченным доступом было бы то, что он не будет подвержен повторной централизации, имеющей место в публичных блокчейнах из-за использования аутсорсинга (economy of scale) и концентрации вычислительных мощностей в руках ограниченного круга лиц» .

Согласно Шеридану, алгоритм консенсуса будет похож на тот, что используется в Биткойне, требуя, чтобы любые изменения, внесенные в блокчейн, были одобрены большинством участников. Чем больше организаций и учреждений будет участвовать в проекте, тем более защищённым будет блокчейн.

По этой причине проект ARCHANGEL задумывается как многосторонний и, возможно, даже международный блокчейн. К осени архивное ведомство надеется привлечь в проект дополнительных партнеров.

«Я не могу сейчас их назвать, но есть целый ряд учреждений, занимающихся сохранением культурно-исторического наследия, которые хотят сотрудничать с нами», - сообщил Шеридан.

На данном раннем этапе тестирования Национальные Архивы уделяют основное внимание использованию решения ARCHANGEL для архивирования изначально-электронных документов, в частности, данных научных исследований и видеозаписей заседаний Верховного суда Великобритании. В дальнейшем ожидается расширение сферы охвата проекта.

«Эти варианты использования мы считаем интересными и важными. Если задачу удастся решить для этих, достаточно сложных материалов, то тогда справиться с такими материалами, как электронная почта или типичные офисные документы ... будет сравнительно легко», - пояснил Шеридан.

Хотя Национальные Архивы в посте по поводу проекта на своём блоге (<https://blog.nationalarchives.gov.uk/blog/trustworthy-technology-future-digital-archives/>) написали, что существующие электронные технологии в принципе позволяют злоумышленникам «переписать историю», однако Шеридан отметит, что проект не является попыткой решить какую-либо из существующих проблем необузданной исторической фальсификации - практики, которая, по его мнению, не является широко распространенной. Скорее, это попытка поддержать ныне существующий уровень доверия

граждан к архивам и учреждениям, сохраняющим культурно-историческую память.

Однако даже если проект окажется выполнимым и все технические проблемы будут решены, его успех зависит от того, подходит ли данное технологическое решение для принципиально психологической проблемы: обеспечения доверия.

«Речь идет о поддержании в будущем существующего высокого уровня доверия к нам. В том будущем, в котором уровень доверия людей, особенно к электронным доказательствам в любой форме, будет постоянно падать».

Однако предлагаемые архивной службой дополнительные меры могут обеспечить стабильное доверие только в том случае, если широкая общественность поймет эту технологию и её удастся убедить (то есть сможет **доверять**), что данная технология действительно надёжно защищена от несанкционированного доступа, как утверждает Шеридан. На данный момент технология блокчейна остается относительно неясной и непонятной.

Как отмечает Шеридан, «Мы знаем, что большинство людей не понимает, что такое блокчейн, поэтому слова типа: *«Эй, смотрите, наши документы зафиксированы в блокчейне, поэтому Вы можете доверять им»* мало что значат для многих пользователей наших коллекций».

«Нам следует поэкспериментировать с тем, как лучше донести это [понимание достоинств блокчейна] до пользователей».

ЗМІСТ

Передмова.....	1
Есть ли будущее у микрографии.....	3
Информационная безопасность предприятия: теоретико-методологические основы правового обеспечения.....	6
«Режим конфиденциальности» электронной почты GMail.....	13
Франция: Опубликован порядок оказания услуг «электронного сейфа».....	14
Конференция Инфодокум-2018 «Цифровая экономика».....	17
<u>ИСО: Готовится стандарт PDF/R для хранения и передачи растровых изображений</u>	18
Штат Виктория, Австралия: Онлайн-решение ORDA для разработки и актуализации указаний по срокам хранения и действиям по их истечении.....	21
ИСО: Технический отчет по микроклимату среды хранения архивно-библиотечных материалов.....	24
Консорциум Всемирной паутины W3C выложил проект пересмотренной версии публикации «Недостатки CAPTCHA в плане обеспечения доступности».....	26
Фонд «Открытая сохранность» опубликовал свою новую стратегию на 2018 – 2021 год.....	28
Хорватия: Принят новый закон об архивных материалах и архивах...	30
Евросоюз: Опубликованы новые стандарты семейства LOTAR.....	32
Новая эра сотрудничества в проведении исследований в области обеспечения долговременной сохранности электронных материалов.....	34
Национальные Архивы Великобритании тестируют использование блокчейна для целей обеспечения долговременной сохранности исторических документов.....	38