ПЕРЕДМОВА

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

У публікації «Жизни потеряны, миллиарды потрачены впустую из-за провалов в управлении государственными документами» розповідається про те, що сертифіковані Пентагоном додатки повинні були вирішити проблему управління електронними документами. Замість цього вони дали лише трохи більше, ніж ілюзію, оскільки переважна більшість цих додатків ніколи не впроваджується, трудовитрати, необхідні для ручного введення в них кожного документа, є непідйомними. Все це триває майже чверть століття. Незважаючи на це, Управління загальних служб уряду США переуклало контракт на «Корпоративні офісні рішення оборонної галузі» з пакетом хмарних послуг, що включає DoD-сертифікований компонент, - на суму 7,6 мільярда доларів.

У публікації «Совместное заявление МСА и ИФЛА по поводу влияния законодательства о защите персональных данных на архивное дело» наведено текст Заяви Міжнародної ради архівів (МСА) і Міжнародної федерації бібліотечних асоціацій і установ (ІФЛА) про законодавство з питань захисту недоторканності приватного життя і архівування.

У публікації «ИСО/МЭК: Опубликована третья редакция руководства по аудиту систем менеджмента информационной безопасности» в якій містяться рекомендації по менеджменту програми аудиту системи менеджменту інформаційної безпеки (СМІБ), з проведення аудитів і за компетенцією аудиторів СМІБ, – на додаток до рекомендацій, що містяться в стандарті ISO 19011: 2018 «Керівництво з аудиту систем менеджменту».

У публікації «Опубліковано перший міжнародний стандарт щодо вирішення питань управління конфіденційною інформацією» в якому формуються вимоги до створення, впровадження, підтримання та постійного вдосконалення системи управління інформаційною безпекою, пов'язаною з конфіденційністю.

У публікації «Италия: Использование блокчейна для обеспечения электронной сохранности согласно требованиям национального регулятора Agid – сценарий будущего» розповідається, що блокчейн на сьогоднішній день жодним чином не може бути використано для процесів забезпечення електронного збереження відповідно до законодавства і, отже, не може використовуватися для збереження в часі юридичної сили відповідно до положень «Кодексу електронного уряду».

У публікації «Франция: Серия обучающих семинаров «Новые парадигмы архивного дела и управления документами»» розповідається про серію відкритих семінарів, спільно організованих лабораторією «Інформаційно-комунікаційні системи в цифрову епоху» при Національній консерваторії мистецтв і ремесел, Національним архівом і центром ім. Жана Мабійона при

Національній школі хартій, в рамках Центру компетенцій в області історії і антропології знань, методик і переконань.

У публікації «ИСО: Опубликован стандарт ISO 22396:2020 «Жизнестойкость сообществ - Руководство по информационному обмену между организациями»» наведено зміст рекомендації щодо обміну інформацією. Цей стандарт включає в себе принципи, рамкову структуру і процес обміну інформацією. Документ визначає механізми обміну інформацією, які дозволяють вчитися на чужому досвіді, помилках і успіхах. Він може використовуватися в якості керівництва при підтримці механізму обміну інформацією з метою підвищення зацікавленості і залучення. Передбачає заходи, які підвищують здатність організації приймати участь справлятися з ризиком перебоїв в її діловій діяльності.

У публікації «Роберт Блатт: Надежны ли технологии облачного хранения для документов, критически-важных для выполнения организацией её миссии?» наведено переклад замітки Роберта Блатта, відомого американського консультанта, на статтю Лючіани Дюранті під назвою «Забезпечення довготривалого збереження в хмарі: Як будуть виглядати в майбутньому заслуговуючи на довіру системи забезпечення збереження?» з коментарями.

У публікації «Новый европейский стандарт EN 17529 «Запроектированная и по умолчанию защита персональных данных и неприкосновенности частной жизни»» запропоновано розробникам компонентів і підсистем формалізований процес виявлення об’єктів та вимог по захисту недоторканості особистого життя.

ЖИЗНИ ПОТЕРЯНЫ, МИЛЛИАРДЫ ПОТРАЧЕНЫ ВПУСТУЮ ИЗ-ЗА ПРОВАЛОВ В УПРАВЛЕНИИ ГОСУДАРСТВЕННЫМИ ДОКУМЕНТАМИ

Источник: сайт издания «The Epoch Times» https://www.theepochtimes.com/the-illusion-of-transparency_3234958.html

Человек, который в 2017 году расстрелял 26 человек в одной из церквей Техаса, использовал для этого оружие, которое он не смог бы купить, если бы американские ВВС должным образом управляли своими документами.
В шести эпизодах чиновники военного ведомства так и не отправили в ФБР документы на Девина Келли (Devin Kelley) в тот период, когда военно-воздушные силы проводили расследование в его отношении, отдали его под военный трибунал и посадили в тюрьму за жестокое обращение с женой и пасынком. Если бы ФБР получило эти документы, будущему убийце было бы запрещено покупать оружие, использованное в этой бойне.

Хотя эта история с участием ВВС может показаться уникальной, сбои в управлении федеральными документами скрываются за рядом самых больших сенсаций последних лет. Масштабы крупнейшей в истории Соединенных Штатов утечки информации из государственных систем, имевшей место в 2015 году, особенно ярко характеризует количество документов, похищенных из Департамента управления персоналом (Office of Personnel Management, OPM – *независимое агентство правительства США, управляющее системой государственной службы*) – 21,5 миллиона. Подобные провалы фигурировали в скандале с Налоговой службой (Internal Revenue Service, IRS), которая целенаправленно проводила аудит консервативных по своей политической ориентации групп, а также в истории с несанкционированным использованием частного почтового сервера тогдашним государственным секретарём Хиллари Клинтон.

По мнению двух экспертов, имеющих несколько десятилетий опыта применения стандарта для систем управления электронными документами, лежащего в основе практически всего программного обеспечения для управления документами, развёрнутого в федеральных органах исполнительной власти, – вполне предотвратимые сбои, которые, среди прочих факторов, сделали возможной резню в городе Сазерленд-Спрингс, штат Техас, являются не столько аномалией, сколько симптомом огромной по масштабам проблемы, охватившей все органы федерального правительства.

Целевая группа (*Объединённая группа проверки взаимодействия систем - Joint Interoperability Test Command, JITC*) при Агентстве оборонных информационных систем (Defense Information Systems Agency, DISA) Министерства обороны США в 1995 году разработала стандарт DoD 5015.2 «Требования к проектированию электронных систем управления документами» (Electronic Records Management Software Applications Design Criteria). Три года

спустя Национальные Архивы США одобрили использование этого стандарта всеми федеральными органами исполнительной власти. В течение последующих двух десятилетий правительство потратило миллиарды долларов налогоплательщиков на приложения для управления документами, сертифицированные на соответствие этому стандарту.

Но эти деньги в значительной степени были потрачены впустую, поскольку на рубеже веков эти приложения стали непригодными к использованию по мере того, как развитие технологий открыло новую эру взаимосвязанных электронных рабочих пространств, переполненных документами, которыми нужно управлять. Приложения эпохи 1990-х годов требуют, чтобы каждый государственный служащий вручную регистрировал в системе каждый документ. Когда объёмы и разнообразие документов стремительно увеличились, такая задача стала неподъёмной.

Важно понимать, что наряду с развитием технологий, большую роль сыграло изменение национального законодательства: если ранее полноценными доказательствами признавались лишь «официальные» документы», которым такой статус устанавливали сами организации, то примерно с 2006 года к ним фактически была приравнена любая документированная информация, и в первую очередь сообщения электронной почты.

Наличие обязательного для некоторых (но далеко не для всех!) ведомств стандарта фактически позволило государственным органам без дополнительных затрат получать решения с более богатым набором функциональных возможностей.

Дэрил Прескотт (Daryll Prescott) возглавлял целевую группу DISA, занимавшуюся с 1993 по 1995 год разработкой стандарта для систем управления электронными документами. Об этих проблемах ему стало известно в начале 2000-х годов.

«Люди заняты основной работой. У них нет времени на то, чтобы перетаскивать электронные объекты по папкам», – говорит Прескотт. «Миллиарды были потрачены на приложения для управления документами, которые не работают, и которыми люди не пользуются. Это плохая услуга для граждан Соединенных Штатов и для специалистов данной отрасли».

Дон Людерс (Don Lueders), бывший федеральный подрядчик, взаимодействовавший с IBM и другими компаниями-разработчиками программного обеспечения, два десятилетия занимался разработкой и продажей приложений для управления документами, основанными на стандарте Министерства обороны США (DoD). У него часто была возможность воочию убедиться, действительно ли используются закупленные государственными органами приложения.

Дон Людерс, бывший подрядчик государственных органов и сертифицированный специалист по управлению документами, на фоне здания Национальных Архивов в Вашингтоне 8 февраля 2020 года. (Фото: Samira Bouaou/Epoch Times)

По словам Людерса, эти приложения никогда толком не использовались, в том числе в Министерстве юстиции (Department of Justice), Государственном департаменте, Министерстве финансов (Department of Treasury), Налоговой службе (IRS) и во многочисленных структурных подразделениях Министерства обороны США, таких, как Отдел связи Белого дома (White House Communications Agency, WHCA - отдел военного управления Белого дома; обеспечивает работу систем правительственной связи, в том числе секретность переговоров).

«Я обучал их применению, консультировал по ним. Я заработал на этом много денег», - говорит Людерс. «Примерно семь или восемь лет тому назад я пришёл к выводу, что больше не могу поддерживать этот стандарт. И я больше не мог его поддерживать, потому что знал, что не только я никогда не видел, чтобы документ из среды деловой деятельности попадал в DoD-сертифицированное хранилище; я даже никогда не видел ни единого успешного развёртывания этих приложений. Все они пустые».

Один бывший высокопоставленный чиновник Пентагона сказал изданию «The Epoch Times», что за весь десятилетний период своей работы в Министерстве обороны он никогда не использовал приложение для управления документами. Его практика управления документами сводилась исключительно к размещению файлов в папках на дисках выданного ему служебного компьютера, что очень далеко от сложных процедур регистрации, хранения, отслеживания сроков хранения и уничтожения, заложенных в программные приложения для управления документами, использование которых каждым сотрудником Пентагона было обязательно согласно нормативным документам.

«Сотрудники не получают поощрений за управление документами», – отмечает этот чиновник, согласившийся беседовать на условиях анонимности. «Я никогда не получал бонусов за надлежащую работу с документами. Вас вознаграждают за продуктивную работу по вопросам, являющимся

актуальными для руководства. Когда я вышел на пенсию и ушёл с государственной службы, мои документы, вероятно, не сохранились».

Бывший специальный агент ФБР Марк Раскин (Marc Ruskin) также подтвердил нашему изданию, что он никогда не использовал специализированных приложений для управления какими-либо документами из тех, что он создавал или получал в течение двух десятилетий работы в ФБР.

Он вспомнил о неудачной попытке внедрения приложения для управления документами в 2004-2005 годах, в период, когда директором ФБР был Роберт Мюллер (Robert Mueller). После того, как это программное обеспечение было выброшено на свалку, ФБР начало работу по развертыванию новой системы. Раскин никогда не использовал новое программное обеспечение вплоть до своего ухода с работы семь лет спустя, несмотря на то, что он прошёл соответствующее обучение.

«В период руководства Мюллера был большой провал с переходом на безбумажные технологии», – говорит Раскин, который также является одним из авторов «The Epoch Times». «Мюллер напористо пытался оцифровать всё и вся. ФБР попыталась перейти на систему, которая не была полностью разработана – это было что-то вроде бета-версии, и не готова к использованию. Ни у кого не хватило смелости сказать директору, что они не смогут уложиться в намеченные им сроки».

В течение последних семи лет были опубликованы переводы ряда заметок Дон Людерса :

- «Дон Людерс: Почему я больше не поддерживаю стандарт DoD 5015.2», https://rusrim.blogspot.com/2013/06/dod-50152.html
- «Дон Людерс: Управление документами после DoD 5015.2 – Девять грядущих изменений», https://rusrim.blogspot.com/2014/07/dod-50152.html
- «Что наболело на душе у наших американских коллег? Открытое письмо Дона Людерса международной ассоциации специалистов по управлению документами и информацией ARMA International», https://rusrim.blogspot.com/2016/04/arma-international.html
- «Комментарии Вики Лемьё по поводу управления документами и блокчейна», https://rusrim.blogspot.com/2016/09/blog-post_35.html
- «США: Управление документами следующего поколения пришло в федеральные органы», https://rusrim.blogspot.com/2017/12/blog-post_21.html и https://rusrim.blogspot.com/2018/04/2_17.html

Также Дон Людерс упоминается в других постах:

- «Интервью Рендольфа Кана блогу «Управление документами следующего поколения» о «защитимом уничтожении»», https://rusrim.blogspot.com/2014/06/1.html

«США: Развенчание мифа о необходимости сертифицировать системы для управления документами на соответствие стандарту DoD 5015.2», https://rusrim.blogspot.com/2014/08/dod-50152-1.html

Основа подотчётности

Несмотря на свое скучное название, управление документами лежит в основе взаимоотношений правительства с американским народом, который его финансирует. Текущий социальные контракт основан на подотчётности и прозрачности, которые невозможно обеспечить без документов. Взрывной рост объёмов документов, сопровождавший бум информационных технологий, значительно сократил способность правительства быть подотчётным и прозрачным.

Теоретически сертифицированные Пентагоном приложения должны были решить эту проблему. Вместо этого они дали лишь немногим большее, чем иллюзия управления документами, поскольку подавляющее большинство этих приложений никогда не внедряется.

«Без подотчётности и прозрачности у Вас нет демократии», – подчёркивает Людерс. «У Вас нет подотчётности и прозрачности без управления документами».

В отсутствие эффективной системы сохранения, защиты, отслеживания и, – когда это требуется по закону, – уничтожения документов, возникающий хаос передаёт власть над государственными документами карьерным администраторам, которые могут выбирать, какие из документов «увидят свет дня», а какие просто исчезнут.

«Всё это продолжается почти четверть века», – говорит Людерс. «И не имеет значение, кто сидит в Белом доме. Я наблюдал это собственными глазами в федеральных органах исполнительной власти. Информация сейчас является самой ценной валютой в мире, и эти люди контролируют информацию».

«Таким образом, они могут безнаказанно делать и говорить всё, что хотят. Мысль об этом ужасает».

Проигнорированное решение

После разработки стандарта DoD 5015.2, Прескотт в значительной степени отошел от отрасли управления документами, пока в 2003 году ему не позвонил тогдашний Архивист США Джон Карлин. В рамках одной из инициатив президента Джорджа Буша Национальные Архивы намеревались разработать и внедрить политики, регламентирующие хранение федеральных электронных документов. Прескотт прошёл собеседование и в 2004 году начал работать в Национальных Архивах в качестве прикомандированного сотрудника. Он возглавлял межведомственные усилия по созданию нового, основанного на услугах стандарта для управления документами, который позволил бы правительству догнать быстрый прогресс в технологиях.

Спустя четыре с половиной года совместные усилия 19 ведомств, возглавляемые Прескоттом, привели к созданию нового стандарта. В нём были установлены требования к службам управления записями (records management services, RMS), которые должны были справиться с неподъёмным бременем ручной работы, налагаемым на конечных пользователей сертифицированными по DoD приложений.

Когда в 1998 году Национальные Архивы поддержали стандарт DoD 5015.2, у крупных технологических компаний сразу же возникла экономическая заинтересованность в разработке соответствующих критериям правительства продуктов, поскольку это гарантировало успешные продажи. Прескотт знал, что то же самое произойдёт, если Национальные Архивы одобрили новый стандарт RMS. В ожидании такого одобрения, две технологические компании обратились к его команде, представив прототипы, основанные на описанных ими услугах.

Но прежде, чем было создано работающее решение, Национальные Архивы ушли от нового стандарта.

«Остается вопрос: почему?», - говорит Прескотт.

Records Management Services (RMS)

Version 1.0

Прескотт передал новый стандарт «Группе управления объектами» (Object Management Group, OMG, https://www.omg.org/) – международному консорциуму по технологическим стандартам. OMG использовал стандарт для создания высокоуровневых моделей, которые могут быть применены для создания поддерживающего RMS программного обеспечения для любой системы.

После того, как консорциум OMG опубликовал стандарт в ноябре 2011 года (*см.* https://www.omg.org/spec/RMS/1.0/ , *прямая ссылка* https://www.omg.org/spec/RMS/1.0/PDF), Ларри Джонсон, в настоящее время входящий в Совет директоров OMG, представил его Национальным Архивам. К его удивлению, Национальные Архивы снова не поддержали стандарт.

«Я был в общем-то шокирован», – рассказывает Джонсон. В тот момент Национальные Архивы искали способы исполнения президентского меморандума об управлении государственными документами, выпущенного президентом Бараком Обамой (Barack Obama) в конце 2011 года. Стандарт RMS отвечал практически всем требованиям Обамы, однако Национальные Архивы не проявили к нему интереса.

«Я был несколько озадачен столь холодной реакцией», – вспоминает Джонсон. Национальные Архивы не ответили на наш вопрос о том, почему стандарт RMS так и не был ими поддержан.

Несмотря на потраченные на приложения для управления документами миллиарды долларов, федеральное правительство сегодня оказалось в тупике, не зная, что делать с непригодным для использования программным обеспечением.

«Плох не стандарт, а системы», - отмечает Прескотт. «Приложения просто не подходят для текущих условий».

Неравнодушный активист

Людерс первоначально рассказал о своей озабоченности несколько лет тому назад в своём отраслевом блоге и в социальных сетях Затем он забил тревогу в IBM, где работал в составе команды, продающей программное обеспечение для управления документами органам федерального правительства.

Видя, что IBM не собирается что-либо предпринимать, Людерс в мае 2017 года подал официальную жалобу генеральному аудитору Министерства обороны. Тот переслал жалобу своему коллеге в DISA, который месяц спустя побеседовал с Людерсом. Генеральный аудитор DISA отказался проводить расследование и перенаправил жалобу в Объединённую группу проверки взаимодействия систем Министерства обороны для рассмотрения в качестве бизнес-проблемы.

Фирма IBM не ответила на просьбу нашего издания дать свои комментарии.

В июле 2017 года Людерс подал еще одну жалобу на имеющиеся нарушения генеральному аудитору разведывательного сообщества США, но так и не получил ответа. Подозревая, что и здесь его жалобу расследовать не станут, он вышел на контакт с офисом тогдашнего члена Палаты представителей Конгресса США от его округа Барбары Комсток (Barbara Comstock, от Республиканской партии, штат Вирджиния), и поддерживал его до того момента, когда сотрудники Комсток внезапно оборвали связь. Комсток потеряла свое место в Конгрессе в ноябре 2018 года. На запрос нашего издания о комментариях Комсток не ответила.

Приложения, разработанные с целью соответствовать стандарту Пентагона, поддерживают функциональные возможности, имеющие ключевое значение для обеспечения прозрачности и подотчётности правительства. Они требуют от каждого государственного служащего регистрировать документы в сертифицированной системе, обеспечивающей защиту документа и невозможность его удаления или изменения.

Документы, подлежащие уничтожению по истечении определенного времени, удаляются приложением с использованием надёжных, подтверждённых цифровой криминалистикой методов, поэтому впоследствии их невозможно восстановить. По словам Людерса и Прескотта, это уже должно было произойти со значительной частью из 21,5 миллионов документов,

украденных из Департамента управления персоналом (Office of Personnel Management, OPM – независимое агентство правительства США, управляющее системой государственной службы) начиная с 2015 года. Если бы документы находились в хранилище системы управления документами, сертифицированной на соответствие стандарту DoD, или же управлялись в соответствии со стандартом RMS, то программное обеспечение уничтожило бы значительную их часть в соответствии с федеральными законами и нормативными актами задолго до того, как кибератака, предположительно инициированная из Китая, привела к взлому информационных систем OPM.

Защита и неизменность документов, которые не подлежат уничтожению или изменению, обеспечивается в случае их регистрации в приложении. Именно так должно было бы обстоять дело с электронными письмами одной из руководителей Налоговой службы Луи Лернер, которая оказалась в центре скандала, связанного с «повышенным вниманием» службы к консервативным группам. Однако Налоговая служба (IRS) утверждала, что электронные письма, которые подлежали раскрытию в соответствии с требованием на выемку документов, выданным Конгрессом, были утрачены из-за компьютерного сбоя. Позднее IRS уверяла, что электронная переписка ещё пяти чиновников отсутствовала вследствие компьютерных сбоев. Эти электронные письма не были бы потеряны, если бы Лернер и другие официальные лица использовали приложение для управления документами.

Нежизнеспособный стандарт

Неспособность правительства использовать сертифицированные приложения коренится в самой природе стандарта DoD. Прескотт разработал этот стандарт в офисе помощника министра обороны по вопросам командования, управления, связи и разведки в 1990-х годах в качестве реакции на сбои в управлении документами, выявленные в ходе попыток федерального правительства собрать данные о военнослужащих, ставших жертвой «синдрома войны в Персидском заливе» (https://www.military.com/benefits/veterans-health-care/gulf-war-syndrome.html). Прескотт работал над стандартом с 1993 по 1995 год. Министерство обороны опубликовало первую версию стандарта в 1997 году.

За прошедшие с тех пор 23 года стандарт дважды обновлялся, но ни одно из внесённых изменений не привело его в соответствие с ошеломляющим технологическим прогрессом, достигнутым с 1995 года. Суть проблемы заключается в том, что стандарт регламентирует создание приложений, требующих скорее ручного ввода, чем услуг и сервисов, которые бы справились с этой работой в фоновом режиме. Подавляющее большинство приложений для управления электронными документами в государственных органах и учреждениях остаются неиспользуемыми, поскольку трудозатраты, необходимые для ручного ввода в них каждого документа, являются неподъёмными.

«Вы создаёте иллюзию [управления документами], которая не совпадает с реальностью», – говорит Прескотт. «Это не соответствует потребностям нашей республики».

Стандарт DoD не содержит требований к удобству использования. Юристы проверили стандарт на соответствие установленным Конгрессом законодательным требованиям к управлению документами (https://www.law.cornell.edu/uscode/text/44), а также нормативным актам исполнительной власти. Удобство использования и жизнеспособность не были частью этого процесса.

«Никто, – включая целевую группу, – не тестировал эти решения с тем, чтобы посмотреть, действительно ли они будут работать в среде промышленной эксплуатации», – отмечает Людерс. «Они и не работают».

Прескотт, во время работы в качестве прикомандированного к Национальным Архивам специалиста, отметил в своей презентации (https://www.powershow.com/view1/1eabd0-ZDc1Z/Daryll_Prescott_powerpoint_ppt_presentation), что приложения для управления документами «должны быть вставлены в бесчисленное число мест в бизнес-процессах» и что они «никогда не отвечали требованиям, изначально сформулированным в 1990-х годах».

В качестве примера усилий, связанных с регистрацией отдельного документа, государственный чиновник, который отправляет электронное письмо, должен определить, основываясь на знаниях, полученных в ходе обучения вопросам управления документами, вообще является ли это электронное письмо государственным документом. Затем он должен перетащить электронное письмо из ящика исходящей переписки в приложение для управления документами и заполнить такие метаданные (*карточку документа*), как гриф секретности и дата истечения срока хранения, после которой документ может быть уничтожен. Это должно быть сделано для каждого документа, будь то электронное письмо, текстовое сообщение, пост в социальной сети, текстовый документ, электронная таблица, запись в календаре, или любой другой иной признаваемый документом объект.

«Вам всегда не хватает времени на основную работу. Если Вы попробуете сказать, что не успеваете сделать порученное потому, что следуете стандарту документирования, Вас сочтут сумасшедшим», – говорит бывший высокопоставленный руководитель Министерства обороны.

Фирма IBM взяла Людерса на работу в 2015 году после того, как он стал громким критиком провалов, связанных с ограниченностью программных приложений. Людерс объясняет, что согласился на это предложение, поскольку фирма IBM заявила о своей заинтересованности в разработке решения, не связанного со стандартом DoD. Когда же он обнаружил, что IBM продолжает продавать программное обеспечение, основанное на всё том же стандарте, он стал на это жаловаться, и в итоге ему пришлось уйти.

«Хранитель документального наследия нации»

Несмотря на одобрение, начиная с 1998 года, стандарта DoD для всех федеральных органов исполнительной власти, Национальные Архивы США

(NARA), именующие себя «хранителем документального наследия нации», сами используют сертифицированное на соответствие стандарту приложение только для своих документов в электронной почте.

«Национальные Архивы признают, что единое решение на все случаи жизни, покрывающее все потребности государственного органа в управлении электронными документами, как правило, оказывается непрактичным», – заявил нашему изданию в своем электронном письме пресс-секретарь Национальных Архивов.

По словам Национальных Архивов, они управляют остальными своими документами «в тех системах, в которой они созданы, причём действия по истечении сроков хранения могут выполняться как вручную, так и с применением автоматизированных методов». Ведомство не отреагировало на просьбу объяснить, какие процессы и политики применяются для удовлетворения обширных федеральных требований к управлению электронными документами, включая вопросы регистрации документов, обеспечения их неизменности, управления на основании указаний по срокам хранения и действиям по их истечении, и, при необходимости, уничтожения без возможности восстановления.

В 2017 году Национальные Архивы выпустили руководство, разъясняющее, что соблюдение стандарта DoD 5015.2 обязательно только для структур Министерства обороны. В 2018 году Национальные Архивы опубликовали собственный набор «Универсальных требований к управлению электронными документами» (Universal Electronic Records Management Requirements, см. https://www.archives.gov/records-mgmt/policy/universalermrequirements - «Эти требования не зависят от конкретного подхода или инструмента, что даёт федеральным органам исполнительной власти поставщикам большую гибкость при поиске отвечающих требованиям NARA решений для управления документами», – добавил пресс-секретарь Национальных Архивов.

Несмотря на недавние перемены в Национальных Архивах, DoD-сертифицированные приложения остаются предпочтительным для многих государственных органов программным обеспечением, отчасти потому, что этот стандарт – единственный, который прямо упомянут в федеральном законодательстве (см. https://www.law.cornell.edu/cfr/text/36/1236.20) по вопросам управления электронными документами.

Расходы для налогоплательщиков

Трудно оценить общие затраты налогоплательщиков за два десятилетия развертывания нежизнеспособного программного обеспечения для управления документами, отчасти из-за плохого управления документами, относящимися к выдаче соответствующих федеральных контрактов. Неисчерпывающий поиск DoD-сертифицированных продуктов позволил выявить контракты стоимостью в десятки миллионов долларов каждый. По словам Людерса, суммарные расходы вполне могут исчисляться миллиардами долларов.

«Если вы сложите все контракты, которые были присуждены потому, что программное решение включало DoD-сертифицированное хранилище, и все услуги по поддержке этих контрактов, Вы довольно быстро получите миллиарды», - подчёркивает Людерс.

По данным консалтинговой компании GEP, занимающейся закупками и поставками, в 2016 году индустрия приложений для управления документами в Соединенных Штатах была оценена в 17–19 миллиардов долларов (https://www.gep.com/mind/blog/trends-records-management). Управление общих служб правительства США (General Services Administration, GSA) недавно перезаключило контракт на «Корпоративные офисные решения оборонной отрасли» (Defense Enterprise Office Solutions) – пакет облачных услуг, включающий DoD-сертифицированный компонент, – на сумму 7,6 миллиарда долларов.

Но истинная цена хаоса, вызванного плохим управлением документами, может быть экспоненциально выше. В 2016 году генеральный аудитор Министерства обороны США выявил, что у Пентагона нет документов для того, чтобы отчитаться о расходах в размере **6,5 триллионов долларов** (https://www.dodig.mil/reports.html/Article/1119298/army-general-fund-adjustments-not-adequately-documented-or-supported/).

«Трагические последствия»

Цена возможностей, упущенных из-за ненадлежащего управления документами, значительна – как, например, в случае тех, кто страдает от «синдрома войны в Персидском заливе». Помимо денег, провалы в управлении документами имеют порой более трагические последствия.

Семьи жертв бойни в Техасе в 2017 году подали против правительства ряд исков, утверждая, что небрежность управления документами в Военно-воздушных силах позволила убийце приобрести использованное им оружие. Впоследствии эти иски были объединены в одно дело. В прошлом году семьи преодолели ключевой барьер, когда федеральный судья Ксавье Родригес (Xavier Rodriguez) разрешил дальнейшие слушания по ряду обвинений в рамках этого дела. Судебный процесс начинается 8 сентября 2020 года.

В своём постановлении Родригес отметил, что Пентагону давно известно о провалах в управлении документами, особенно когда речь идет об уведомлении ФБР о расследовании, судебном преследовании и осуждении военнослужащих. В 2014 году генеральный аудитор Министерства обороны обнаружил, что Служба безопасности ВВС в 60% случаев не передала в ФБР карты с отпечатками пальцев и отчеты об окончательном решении по делам. В 2015 году генеральный аудитор Министерства обороны изучил данную проблему в нескольких видах вооруженных сил и выявил, что ВВС не представили в соответствующие компьютерные базы данных документы о судимости в 30% случаев.

К 2017 году Военно-воздушные силы так и не исправили свои ошибки в управлении документами. Служба аудита выявила, что недостатки в информировании ФБР об уголовных приговорах имели место в 94% случаев. В

отчете отмечалось: «Любые отсутствующие карточка с отпечатками пальцев и отчет об окончательном решении могут иметь серьезные, даже трагические последствия, как это вполне могло случиться в случае недавней стрельбы в церкви в Техасе».

Ни один из отчетов генерального аудитора за 2014, 2015, 2017 и 2018 годы не содержит ни единого упоминания о стандарте DoD 5015.2, который формально регламентирует обработку электронных документов, упомянутых в каждом таком отчете. В случае с Келли военнослужащие ВВС в некоторых случаях просто не смогли найти документы, – которые были бы сохранены, если бы они использовали приложение, сертифицированное по DoD.

К тому времени, когда у ВВС 8 июня 2012 года появилась третья возможность отправить документы Келли в ФБР, ФБР перестало принимать бумажные карты с отпечатками пальцев. В результате карты следовало отсканировать и зарегистрировать как электронные документы в DoD-сертифицированном приложении. Пентагону потребовалось ещё два года на то, чтобы уведомить свой персонал о новом требовании ФБР.

Военно-воздушные силы и генеральный аудитор ВВС отказались отвечать на вопрос о том, почему в отчетах отсутствует анализ соответствия стандарту DoD 5015.2.

Министерство обороны, ВВС и генеральный аудитор ВВС отказались давать комментарии, сославшись на предстоящие судебные разбирательства в отношении семей из Сазерленд-Спрингс.

Адвокат семьи Холкомб (Holcombe), потерявшей в бойне девять своих членов, также отказался от комментариев ввиду предстоящего судебного разбирательства.

Фирма IBM, OPM, Министерство юстиции, Государственный департамент, Казначейство, Бюро по патентам и торговле и Отдел связи Белого дома не ответили на просьбы издания о комментариях.

В отличие от случаев неисполнения законодательно-нормативных требований, вскрытых в отчетах генерального аудитора ВВС, провалы в управлении документами, касающиеся DoD-сертифицированных приложений, связаны не только с федеральным правительством. В случае с IBM, Людерс громко говорил о том, что программное обеспечение не используется. Он сообщил, что фирма продолжала продавать его.

По словам Прескотта, другие технологические гиганты давно знают, что их программное обеспечение для управления документами нежизнеспособно в современных электронных средах.

Впервые для себя фирма IBM объявила о прекращении поддержки одного из своих продуктов для управления документами, сертифицированного на соответствие стандарту DoD 5015.2 в апреле этого года.

СОВМЕСТНОЕ ЗАЯВЛЕНИЕ МСА И ИФЛА ПО ПОВОДУ ВЛИЯНИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА АРХИВНОЕ ДЕЛО

Источник: сайт МСА https://www.ica.org/en/ifla-ica-statement-on-privacy-legislation-and-archiving
https://www.ica.org/sites/default/files/statement_on_privacy_legislation_and_archiving_rights_final_en.pdf

3 марта 2020 года Международный совет архивов (МСА) и Международная федерация библиотечных ассоциаций и учреждений, ИФЛА (International Federation of Library Associations and Institutions, IFLA) выпустили совместное заявление, в котором рассказали о своей позиции в отношении защиты персональных данных применительно к архивным документам (IFLA-ICA Statement on Privacy Legislation and Archiving). Заявление было опубликовано на сайте МСА.

Следует отметить, что международное профессиональное сообщество давно уже просило представляющее его интересы ассоциации чётко высказаться на эту тему и донести своё видение до национальных и транснациональных законодательных органов.

Данное 3-страничное заявление доступно на сайте МСА в виде PDF-файла по адресу https://www.ica.org/sites/default/files/statement_on_privacy_legislation_and_archiving_rights_final_en.pdf

Заявление ИФЛА-МСА о законодательстве по вопросам защиты неприкосновенности частной жизни и архивировании

В последние годы наблюдается растущий интерес и поддержка законодательства и судебной практики, направленных на защиту персональных данных. Это является следствием осведомленности об инвазивной, нарушающей неприкосновенность частной жизни природе новых способов сбора и использования персональных данных.

Подобное развитие событий можно в целом приветствовать, однако возникает обеспокоенность по поводу того, влияет ли оно и каким образом на архивную деятельность и на целостность фондов организаций (включающих

документы, данные и т.д.). Учитывая стремление тех, кто занимается управлением архивными материалами, соблюдать закон, – отсутствие ясности в данном вопросе может привести к введению чрезмерно ограничительных кодексов практики; что, в свою очередь, может повлиять на комплектование и обеспечение сохранности архивных материалов и, в конечном итоге, на доступность информации.

Данное заявление направлено на то, чтобы изложить основные принципы, на основе которых библиотеки, архивы и их ассоциации могли бы строить свою идейно-пропагандистскую работу, связанную с законодательством о защите персональных данных.

Природа архивных материалов

Согласно определению, данному Международным советом архивов, архивные материалы являются «документальным побочным продуктом человеческой деятельности, сохраняемым ввиду их долговременной ценности. Они представляют собой оперативные (contemporary) документы, создаваемые отдельными лицами и организациями по мере ведения ими своей деловой деятельности, и, следовательно, позволяют получить непосредственное представление о прошедших событиях» (см. https://www.ica.org/en/what-archive).

Эти материалы обеспечивают фундамент для понимания нашего прошлого, будь то для целей исследований, прозрачности и подотчетности, или же просто для обеспечения максимальной полноты исторических сведений. Как таковые, они помогают строить более крепкие общества и демократии.

Материалы такого рода могут храниться в различных организационно-правовых условиях, в том числе в библиотеках, архивах и музеях. Отбирая, обеспечивая сохранность и предоставляя доступ, учреждения, в которых хранятся архивные материалы, играют важную роль в достижении общественных и гражданских целей.

Архивные материалы и персональные данные

Архивные материалы неизбежно содержат персональные данные, которые можно определить как любую информацию, которая может быть ассоциирована с известным человеком, и которая что-либо раскрывает в отношении его личности, обстоятельств и действий.

Ставшее своего рода эталоном общеевропейское законодательство, вообще говоря, защищает персональные данные только живущих лиц. Защиту персональных данных умерших обеспечивают далеко не все страны, а те, что её предоставляют, делают это по-разному.

Однако для реализации любого режима доступа необходимы функции менеджмента информации и обеспечения её долговременной сохранности, поэтому существует необходимость в одинаково надёжных программах управления документами и архивного хранения.

С обработкой такой информации связан ряд ключевых вопросов. Статья 12 «Всеобщей декларации прав человека» предоставляет право на свободу от

произвольного вмешательства в личную и семейную жизнь и от произвольного посягательства на неприкосновенность жилища и на тайну корреспонденции.

В то же время в статье 29 подчеркивается, что «При осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения должного признания и уважения прав и свобод других и удовлетворения справедливых требований морали, общественного порядка и общего благосостояния в демократическом обществе».

Достижение правильного баланса между требованиями этих статей подразумевает взвешенное профессиональное суждение, основанное на этических принципах. Сотрудники библиотек и архивов придерживаются правил поведения, поддерживающих принятие решений относительно того, как они принимают на себя ответственность за такие материалы, приобретают их, управляют ими и предоставляют к ним доступ. В тех случаях, когда имеются значительные объёмы персональных данных, роль архивиста часто заключается в том, чтобы обеспечить безопасность и сохранность до того момента, когда доступ к нему может быть открыт ввиду того, что документ перестал быть «высокочувствительным» и/или индивидуум умер.

Совместное заявление МСА и ИФЛА по поводу влияния законодательства о защите персональных данных на архивное дело, (Существующие практики обеспечения сохранности и доступности архивных материалов)

Этический кодекс ИФЛА (IFLA Code of Ethics for Librarians and other Information Workers, https://www.ifla.org/publications/node/11092), «Заявление ИФЛА о доступе к персональным данным в исторических документах» (IFLA Statement on Access to Personally Identifiable Information in Historical Records, https://www.ifla.org/publications/ifla-statement-on-access-to-personally-identifiable-information-in-historical-records), и «Международный этический кодекс архивистов» МСА (текст на русском языке здесь: https://www.ica.org/sites/default/files/ICA_1996-09-06_code%20of%20ethics_RU.pdf) – все они устанавливают стандарты, поддерживаемые текущей работой соответствующих экспертных комитетов на глобальном и национальном уровнях.

В них используется подход, поощряющий доступность архивных материалов по умолчанию, когда ограничения, которые необходимо ввести, строго основываются на духе и букве применимого законодательства, включая законодательство о защите неприкосновенности частной жизни (персональных данных), которое интерпретируется в соответствии с профессиональным пониманием и суждением.

К числу подобных ограничений несомненно относятся ситуации, когда информация может способствовать краже личности или когда она является несправедливой, не относящейся к делу либо причиняет неоправданный вред (например, в контексте законодательства о «праве быть забытым»).

Хотя названные выше документы допускают, что доступ может быть ограничен при определенных обстоятельствах, они недвусмысленно возражают против необратимого уничтожения или удаления информации, содержащейся в архивных коллекциях. Подобные действия подрывают способности менеджеров архивных коллекций принимать собственные решения о доступе на основе своих собственных суждений.

Рекомендации в отношении законодательства о защите персональных даннях

В тех случаях, когда новые правила предоставляют отдельным лицам право получать доступ, исправлять или требовать изменения либо удаления касающейся их информации, имеющейся в фондах, хранящих архивные материалы учреждений, возникает риск лишить исследователей и других лиц возможности сегодня и в будущем получать доступ к надежным документам в составе полных коллекций, а также риск уменьшения прозрачности деятельности и подотчётности находящихся у власти лиц.

Ввиду этого мы предлагаем правительствам и другим принимающим решения сторонам следующие рекомендации:

- Мы приветствуем законы, предоставляющие людям больше прав и возможностей влиять на то, каким образом информация о них собирается и обрабатывается;
- В подобных правилах следует, тем не менее, обеспечить наличие исключений, дающих возможность профессиональным учреждениям, таким, как библиотеки и архивы, приобретать и сохранять материалы, содержащие персональные данные;
- Хотя правила доступа к архивным материалам должны поощрять их доступность по умолчанию, они также должны допускать применение, при необходимости, исключений в интересах защиты неприкосновенности частной жизни, конфиденциальности, учёта чувствительных вопросов культурного характера (cultural sensitivities) или законной озабоченности в плане безопасности.
- Ни при каких обстоятельствах законы не должны допускать или предписывать уничтожение или изъятие архивных материалов, хранящихся в организациях документального или культурного наследия, которыми эти материалы были отобраны на постоянное хранение и хранятся ввиду их непреходящей культурной ценности.
- Следует оказывать поддержку хранящим архивные материалы библиотекам, архивам и другим учреждениям в разработке строгих и эффективных кодексов этики и применении их при управлении содержащими персональные данные материалами и при принятии решений о доступе к таким материалам.
- Хранящие архивные материалы библиотеки и архивы должны иметь возможность воспользоваться ограничением их ответственности в случае добросовестности их действий.

Существующие практики обеспечения сохранности и доступности архивных материалов

Этический кодекс ИФЛА (IFLA Code of Ethics for Librarians and other Information Workers, https://www.ifla.org/publications/node/11092), «Заявление ИФЛА о доступе к персональным данным в исторических документах» (IFLA Statement on Access to Personally Identifiable Information in Historical Records, https://www.ifla.org/publications/ifla-statement-on-access-to-personally-identifiable-information-in-historical-records), и «Международный этический кодекс архивистов» МСА (текст на русском языке здесь: https://www.ica.org/sites/default/files/ICA_1996-09-06_code%20of%20ethics_RU.pdf) – все они устанавливают стандарты, поддерживаемые текущей работой соответствующих экспертных комитетов на глобальном и национальном уровнях.

В них используется подход, поощряющий доступность архивных материалов по умолчанию, когда ограничения, которые необходимо ввести, строго основываются на духе и букве применимого законодательства, включая законодательство о защите неприкосновенности частной жизни (персональных данных), которое интерпретируется в соответствии с профессиональным пониманием и суждением.

ИСО/МЭК: ОПУБЛИКОВАНА ТРЕТЬЯ РЕДАКЦИЯ РУКОВОДСТВА ПО АУДИТУ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источник: сайт ИСО https://www.iso.org/standard/77802.html https://www.iso.org/obp/ui/#!iso:std:77802:en

Как сообщил сайт Международной организации по стандартизации (ИСО), в январе 2020 года была опубликована третья редакция стандарта **ISO/IEC 27007:2020 «Информационная безопасность, кибербезопасность и защита неприкосновенности частной жизни - Руководство по аудиту систем менеджмента информационной безопасности»** (Information security, cybersecurity and privacy protection - Guidelines for information security management systems auditing) объёмом 47 страниц, см. https://www.iso.org/standard/77802.html и https://www.iso.org/obp/ui/#!iso:std:77802:en .

Стандарт подготовлен техническим подкомитетом ИСО/МЭК JTC 1/SC 27 «Информационная безопасность, кибербезопасность и защита неприкосновенности частной жизни» (Information security, cybersecurity and privacy protection). Он заменит предыдущую редакцию, которая называлась несколько иначе - ISO/IEC 27007:2017 «Информационные технологии – Методы и средства обеспечения безопасности – Руководство по аудиту систем менеджмента информационной безопасности» (Information technology – Security techniques - Guidelines for information security management systems auditing).

Во вводной части документа сказано:

«Настоящий документ содержит рекомендации по менеджменту программы аудита системы менеджмента информационной безопасности (СМИБ), по проведению аудитов и по компетенции аудиторов СМИБ, - в дополнение к рекомендациям, содержащимся в стандарте ISO 19011:2018 «Руководство по аудиту систем менеджмента» (Guidelines for auditing management systems, https://www.iso.org/standard/70017.html и https://www.iso.org/obp/ui/#!iso:std:70017:en).

Настоящий документ адресован тем, кому требуется разобраться или провести внутренний или внешний аудит СМИБ и/или управлять программой аудита СМИБ».

Содержание документа следующее:

Предисловие

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Принципы проведения аудита
5. Менеджмент программы аудита
6. Проведение аудита

7. Компетенции и оценка аудиторов

Приложение А: Руководство по практике аудита систем менеджмента информационной безопасности

Библиография

ОПУБЛІКОВАНО ПЕРШИЙ МІЖНАРОДНИЙ СТАНДАРТ ЩОДО ВИРІШЕННЯ ПИТАНЬ УПРАВЛІННЯ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

Источник: https://sm.od.ua/predpriyatie/pres-tsentr/novosti/619

Останнім часом кібербезпека викликає все більше занепокоєння, оскільки кількість атак на бізнес значно збільшилася і становить все більш серйозну загрозу для глобальної стабільності. Не дивно, що швидко впроваджуються закони і нормативні акти, щоб знизити ці ризики і захистити цифрову конфіденційність.

Нещодавно було опубліковано перший в світі міжнародний стандарт, що допоможе організаціям керувати інформацією про конфіденційність відповідно до нормативних вимог.

Стандарт **ISO/IEC 27701 «Методи і засоби забезпечення безпеки»** можна вважати доповненням до вже існуючих стандартів: ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги» та ISO/IEC 27002 «Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки» для управління інформацією про конфіденційність. Новий стандарт формує вимоги до створення, впровадження, підтримання та постійного вдосконалення системи управління інформаційною безпекою, пов'язаної з конфіденційністю. Іншими словами, створена система управління інформацією для захисту персональних даних (PIMS).

Стандарт ISO/IEC 27701 визначає параметри процесів і забезпечує керівництво для захисту особистої інформації на постійній основі. Система управління інформацією визначає процеси для постійного поліпшення захисту даних, що особливо важливо в світі, де технології не стоять на місці.

Стандарт ISO/IEC 27701 був розроблений технічним комітетом «Безпека інформаційних технологій, кібербезпека і захист даних», який складається з експертів з усього світу, які займаються захистом даних органів безпеки, наукових кіл та представників промисловості.

ИТАЛИЯ: ИСПОЛЬЗОВАНИЕ БЛОКЧЕЙНА ДЛЯ ОБЕСПЕЧЕНИЯ ЭЛЕКТРОННОЙ СОХРАННОСТИ СОГЛАСНО ТРЕБОВАНИЯМ НАЦИОНАЛЬНОГО РЕГУЛЯТОРА AGID - СЦЕНАРИЙ БУДУЩЕГО

Источник: Блог Николя Савино / GoogleDrive
https://www.savinosolution.com/2020/02/05/blockchain-conservazione-digitale-ad-oggi-non-si-puo/
https://drive.google.com/file/d/1TqNIdS_afyWio9tGALgKwtCEv2zM_npA/view

Почему блокчейн не используется для хранения

Несмотря на то, что общих элементов действительно много, блокчейн на сегодняшний день никоим образом не может использоваться для процессов обеспечения электронной сохранности в соответствии с законодательством и, следовательно, не может использоваться для сохранения во времени юридической силы в соответствии с положениями «Кодекса электронного правительства» (Codice dell'Amministrazione Digitale).

Это связано не столько с техническими проблемами, сколько с отсутствием соответствия законодательно-нормативной базы процессным требованиям. Я говорю о процессах, поскольку сегодня обеспечение сохранности, а также то, что уже сказано в текущем проекте руководства, разрабатываемого агентством «Электронная Италия» (L'Agenzia per l'Italia Digitale, AgID), основано на очень важном структурированном стандарте, а именно на стандарте открытой архивной информационной системы OAIS - это стандарт ISO 14721:2012 «Системы передачи данных и информации о космическом пространстве. Открытая архивная информационная система. Эталонная модель» (Space data and information transfer systems - Open archival information system (OAIS) - Reference model), см. https://www.iso.org/standard/57284.html и https://www.iso.org/obp/ui/#iso:std:iso:14721:ed-2:v1:en.

Возможно ли реализовать этот стандарт на блокчейне? Несомненно, да. Это уже сейчас может быть сделано. Это правда, что блокчейн не позволяет хранить в нём сами документы и, соответственно, файлы (такие как PDF или другие), - однако он хранит самый важный элемент документа, а именно, его хеш, а также все другие данные / метаданные, связанные с документом. Поэтому легко себе представить блокчейн, связанный с высокоразвитой документной системой, способной обеспечить управление документами в соответствии с законодательством. Далее, новые правила Евросоюза не исключают блокчейн. Отсюда следует, что невозможность сегодня использования блокчейна для хранения электронных документов является чисто проблемой нормативного регулирования.

Выводы

Если мы посмотрим в будущее, то, с учетом отмеченных выше особенностей и приведенных аргументов, блокчейн может легко заменить текущее сохранение «по Agid», а также список решений, аккредитованных Agid.

Неизвестно, суждено ли в ближайшем будущем исчезнуть аккредитованным Agid системам хранения, но, безусловно, необходимо будет продолжить обсуждение данного вопроса, учитывая также, что всё будет зависеть от воли законодателя легализовать блокчейн с точки зрения требований «Кодекса электронного правительства».

ФРАНЦИЯ: СЕРИЯ ОБУЧАЮЩИХ СЕМИНАРОВ «НОВЫЕ ПАРАДИГМЫ АРХИВНОГО ДЕЛА И УПРАВЛЕНИЯ ДОКУМЕНТАМИ»

Источник: сайт программы «Новые парадигмы архивного дела и управления документами» https://nparchive.hypotheses.org/

«Новые парадигмы архивного дела и управления документами» - это серия открытых семинаров, совместно организованных лабораторией «Информационно-коммуникационные системы в цифровую эпоху – Париж, Иль-де-франс» (Dicen-IDF) при Национальной консерватории искусств и ремесел (Conservatoire National des Arts et Métiers, CNAM, http://www.cnam.fr/ *), Национальными Архивами и центром им. Жана Мабийона (Jean Mabillon) при Национальной школе хартий (Ecole Nationale des Chartes), в рамках Центра компетенций в области истории и антропологии знаний, методик и убеждений (Laboratoire d'Excellence Histoire et anthropologie des savoirs, des techniques et des croyances, Labex haStec,* https://labexhastec-psl.ephe.fr/*).*

Данная программа обучения посвящена проблемам и последствиям использования электронных документов и больших данных для практики архивного дела и управления документами.

Тематика, которую мы предлагаем на 2020 год, связана с новыми парадигмами архивной деятельности и управления документами: это актуальность профессиональных теорий и практик в ситуации, когда особенности электронно-цифровых технологий сталкиваются со спецификой исторической миссии.

Цель программы заключается в том, чтобы согласовать цифровую трансформацию архивов и обработки информации с выполнением исторической миссии и профессиональными традициями действующих лиц, максимально учитывая связанные с архивами и документами соображения и сочетая исследования и профессиональное видение.

Мы стремимся, с одной стороны, на основе истории, миссий, теоретических основ и соответствующей практики определить пределы стандартизации цифровых данных и цифровой обработки в соответствующих контекстах (архивы, библиотеки, управление документами); а с другой - способствовать междисциплинарному и транс-профессиональному диалогу в интересах распространения наиболее инновационных цифровых методов и технологии.

Программа 2020 года

Сессия 1: Данные, метаданные, документы? Проблемы семантики

Архивисты, библиотекари, специалисты по управлению документами, компьютерщики и специалисты по данным, похоже, используют одни и те же слова для обозначения объектов, с которыми они работают. Однако значение каждого из этих слов часто различается в зависимости от профессий, а также от особенностей создания и использования объектов. В ходе данного открывающего программу «круглого стола» мы намерены выявить общие точки зрения и расхождения в интерпретации этих терминов, которые используются всеми, но при этом являются многозначными

Сессия 2: Часть и целое: Агрегирование цифровых данных

Мы предлагаем рассмотреть вопрос, общий для всех, чья деятельность связана с информацией – вопрос агрегации (объединения) цифровых данных и их интерпретации. Мы хотим организовать диалог между историком и аналитиком данных с целью решения следующих вопросов:

- Каков вклад цифровых данных в историю?
- Какие инструменты могут использоваться?
- Как принимать решения об объединении тех или иных типов данных, чтобы в результате сделать их более осмысленными?
- Каковы риски этой практики в плане возможности неправильной интерпретации, какая информация необходима для правильной интерпретации объединённых данных?
- Как повышать осведомленность и обучать молодых исследователей?

В отличие от архивиста, историки сталкиваются с коллекциями, в рамках которых множество документов предварительно упорядочены их создателями, - чей смысл они не знают и чью внутреннюю логику им следует воспринять.

Сессия 3: Искусственный интеллект на службе архивного дела и управления документами, а также анализа архивных документов

Развитие технологий искусственного интеллекта открывает новые возможности для архивно-документационных служб и для архивистов. Мы предлагаем обсудить текущее положение дел, а также связанные с данными технологиями этические и научные проблемы и формы сотрудничества между научно-исследовательскими центрами, архивами и компаниями, занимающимися разработкой алгоритмов.

Мы также рассмотрим алгоритм как архивный документ, обращая внимание, среди прочего, на важность знаний об алгоритмах для понимания социальных реалий, административной практики и т.д.

Сессия 4: Для каких архивов пригодятся «озёра данных»?

В результате выбора Национальным аудиовизуальным институтом (Institut national de l'audiovisuel, INA) архитектуры «озера данных» (lac de données, data lake), данный термин вошёл в терминологию предметной области аудиовизуального культурно-исторического наследия. Мы предлагаем уточнить интерпретацию понятия «озеро данных» и оценить возможность их использования учреждениями, занимающимися сохранением культурно-исторического наследия.

Имеет ли мы дело с прототипом модели, предлагающей идеальное решение в плане хранения больших объёмов данных, - или же с моделью, адаптированной к определенным задачам, определенным типам фондов, определенным объёмам, но «недружественной» в плане использования данных? Речь идет о понимании того, как архитектура хранения данных взаимодействует с профессиональной средой и ожидаемыми вариантами применения, и как она связана с развитием алгоритмов и машинного обучения.

Сессия 5: Этнологический взгляд на мутации в профессии и практике архивного дела и управления документами

Исследователи наблюдают за профессионалами архивного дела и управления документами. Они ставят вопросы об актуальности этих профессий, о выполняемой ими роли посредника и об их взаимоотношениях с окружающей средой, пользователями, учреждениями. Ставится вопрос о том, что публика неверно воспринимает эти «невидимые» профессии, не понимая, какую работу на самом деле выполняют их представители. Мы поговорим о том, какие ключевые аспекты профессиональной идентичности сохранятся в процессе цифровых мутаций.

Сессия 6: Аудио- и видеоархивы

Будет рассмотрен вопрос архивации цифровых аудиовизуальных файлов в различных профессиональных и организационных условиях, и почему методы обработки не могут быть одинаковыми. Мы сопоставим различные точки зрения на практику работы.

ИСО: ОПУБЛИКОВАН СТАНДАРТ ISO 22396:2020 «ЖИЗНЕСТОЙКОСТЬ СООБЩЕСТВ - РУКОВОДСТВО ПО ИНФОРМАЦИОННОМУ ОБМЕНУ МЕЖДУ ОРГАНИЗАЦИЯМИ»

Источник: сайт ИСО https://www.iso.org/standard/50292.html https://www.iso.org/obp/ui/#!iso:std:50292:en

Как сообщил сайт Международной организации по стандартизации (ИСО), в феврале 2020 года был опубликован стандарт **ISO 22396:2020 «Безопасность и жизнестойкость – Жизнестойкость сообществ - Руководство по информационному обмену между организациями»** (Security and resilience - Community resilience - Guidelines for information exchange between organizations) объёмом 19 страниц, см. https://www.iso.org/standard/50292.html и https://www.iso.org/obp/ui/#!iso:std:50292:en .

Стандарт разработан техническим комитетом ISO/TC 292 «Безопасность и жизнестойкость» (Security and resilience).

В аннотации на документ отмечается:

«Настоящий документ содержит рекомендации по обмену информацией. Он включает в себя принципы, рамочную структуру и процесс обмена информацией. Стандарт определяет механизмы обмена информацией, которые позволяют участвующей организации учиться на чужом опыте, ошибках и успехах. Он может использоваться в качестве руководства при поддержке механизма обмена информацией с целью повышения заинтересованности и вовлечения. Он предусматривает меры, которые повышают способность участвующей организации справляться с риском перебоев в её деловой деятельности.

Настоящий документ может использоваться частными и государственными субъектами, которым требуется руководство по созданию условий для поддержки обмена информацией.

Настоящий документ не охватывает технические аспекты, и основное внимание в нём уделяется вопросах методологии».

Содержание документа:

Приложение В: Примеры
Библиография

РОБЕРТ БЛАТТ: НАДЕЖНЫ ЛИ ТЕХНОЛОГИИ ОБЛАЧНОГО ХРАНЕНИЯ ДЛЯ ДОКУМЕНТОВ, КРИТИЧЕСКИ-ВАЖНЫХ ДЛЯ ВЫПОЛНЕНИЯ ОРГАНИЗАЦИЕЙ ЕЁ МИССИИ?

Источник: сайт EID https://eid-documentmanagement.com/are-cloud-storage-technologies-reliable-for-mission-critical-records/

Недавно исследовательская статья Лючианы Дюранти (Luciana Duranti) под названием «Обеспечение долговременной сохранности в Облаке: Как будут выглядеть в будущем заслуживающие доверия системы обеспечения сохранности?» (Preservation in the Cloud: What will a Trustworthy Preservation Systems Look Like in the Future?) была распространена среди членов рабочей группы ISO/TC171/SC2/WG11 «заслуживающая доверия подсистема хранения» (Trustworthy Storage Sub-system).

Статья, доступна по адресу: https://www.researchgate.net/publication/301490516_Building_a_Trustworthy_System_What_will_Trustworthy_Systems_Look_Like_in_the_Future .

Ее подзаголовки:

Облако

Политики

Договорные соглашения

- Право собственности на данные
- Доступность, извлечение и использование
- Отслеживание сроков хранения данных и выполнение установленных действий по их истечении
- Хранение и обеспечение долговременной сохранности данных
- Безопасность
- Локализация и передача данных
- Прекращение оказания услуги, прекращение контракта

Обеспечение долговременной сохранности как услуга в области доверия (Preservation as a Service for Trust, PaaST)

Выводы

Эта статья содержит ценные сведения, связанные с хранением и управлением информацией, которая не является критически-важной, так что организация не понесёт непоправимый ущерб, если эти данные будут взломаны, зашифрованы преступниками либо искажены вследствие некорректной работы служб репликации, несанкционированного доступа или атак криптовымогателей.

Использование технологий облачного хранения хорошо подходит для информации, которой необходимо обмениваться вне организации, но не обеспечивает необходимого уровня защиты критически для миссии организации и относящейся к её деловой деятельности информации, необходимой для обеспечения непрерывности деловой деятельности; а также не является достаточным для защиты контента, который считается конфиденциальным или персональным.

Рост числа атак криптовымогателей на облачные хранилища в 2019 году

Как отмечало в конце прошлого года новостное агентство CNN, 140 местных органов власти только в одних США, полицейские участки и больницы также стали заложниками в результате атак криптовымогателей, многие из которых включали «двойной куш» (double-dipping), когда после уплаты первоначального выкупа злоумышленник требовал дополнительные суммы за то, чтобы не раскрывать выпуск и не распространять данные, собранные до шифрования носителей и данных и т.п. Так что представьте себе степень этих проблем в мировом масштабе.

Число атак криптовымогателей значительно выросло за последние 2 года

1. За последние 2 года значительно выросло число атак криптовымогателей, в том числе на облачные технологии хранения. Специализированным государственным органам в сфере кибербезопасности (в США они называются «сертифицированные аудиторы информационных систем» - Certified Information Systems Auditor, CISA) и частным организациям, таким как EMSISOFT, ITRC и т.д. известны, в частности, следующие варианты:

- **CryptoLocker** – старейшая вариация, известна с 2013 года;

- **WannaCry** – наиболее широко известный криптовымогатель, заразивший 125 тысяч организаций в более чем 150 странах; известны такие его подвиды как WannaCry, Wcry, WanaCryptOr и др.
- **Cerber** – нацелен на Office 365 !!! Распространяется через фишинг, и уже пострадали миллионы пользователей!!
- **Crysis** – шифрует файлы на жёстких и съёмных дисках, распространяется через присоединённые к электронным письмам файлы с «двойными» расширениями;
- **CryptoWall** – включает подвиды CryptoDefense, CryptoBit, CryptoWall 2.0, и др.
- **GoldenEye** – похож на Petya, распространяется посредством «социальной инженерии» (т.е. «развода» - Н.Х.) ;
- **Jigsaw** – самый разрушительный криптовымогатель, шифрующий постепенно уничтожающий данные;
- **Locky** – блокирует компьютер и не даёт возможности его использовать;
- Прочие, в число которых входят: **Petya, NotPetya, TeslaCrypt, TorrentLocker, ZCryptor**, и др.

Ущерб от кибератак в США превысил 7,5 миллиардов долларов в 2010 году.

2. На данный момент действующие в сфере безопасности организации, такие, как EMSISOFT и ITRC, а также различные органы исполнительной власти США, оценивают ущерб от этих атак в более чем 7,5 миллиардов долларов.

3. В той или иной степени были взломаны все поставщики облачных услуг, такие как Amazon и Microsoft, - а также различные кредитные агентства (Experian, Equifax, Transunion), когда использовали облачные технологии. В ряде случаев, освещавшихся в последнее время в прессе, имели место неоднократные взломы.

4. Office 365 стал одной из основных целей для направленного фишинга (spear-phishing) и фишинга в электронной почте. Эти атаки стали довольно успешными и позволили злоумышленникам получить доступ к многочисленным учетным записям, что открыло им доступ к облачному хранилищу документов. Хуже всего то, что отсутствует точный и надежный аудит и/или журналы аудита, которые можно было бы проанализировать.

5. Службы репликации осуществляют копирование на уровне байтов и томов, а не на «уровне документов». Таким образом, любые ошибки в источнике реплицируются. Последствия несанкционированного доступа и/или модификации / удаления также реплицируются, что приводит к потере данных и документов.

Сведения о надёжности облачных технологий должны быть актуальными, чтобы иметь ценность

Данная в статье ссылка на публикацию американского Национального института стандартов и технологий (NIST) старше 7 лет, и она устарела вместе

с большинством цитат и ссылок периода с 2013 по 2018 год, причем большинство из них относятся к периоду 2012–2015 годов (а некоторые - к 1998 году). Это временные рамки, когда облачные технологии только начали становиться популярными, прежде, чем конечный пользователь осознал опасности, связанные с использованием облачных технологий для всего, что не является общедоступным и некритичным для деловой деятельности коммерческих и государственных органов и учреждений в целом. По этой очень простой причине в мире сейчас нет государственных органов, которые бы размещали критически-важную для их миссии или секретную информацию в публичном облаке, поэтому, хотя эта статья интересна, в ней представлено очень искаженное представление о текущей ситуации.

Другие ссылки на OGM, OASIS, InterPARES, PaaST основаны на концепции открытого исходного кода, которая делает эти типы атак более распространенными, способствует увеличению их масштабов и частоты, поскольку эти инструменты облегчают злоумышленникам поиск способов взлома этих технологий.

Расширение технических требований и внедрение заслуживающих доверия решений

Как человек, который тратит немало времени на работу в мире цифровой криминалистики, а также на взаимодействие с государственными органами и учреждениями, внедряющими заслуживающие доверия технологии управления документами, - я принимал участие во многих расследованиях и попытках восстановления данных, в основном безуспешных.

Это ключевые факторы, приведшие к тому, что отрасль управления контентом / документами очень напряжённо занимается разработкой и расширением технических требований, связанных с проектированием, разработкой и внедрением доверенных (trustworthy) решений, защищающих данные с помощью таких инструментов, как модели «Доверенных подсистем хранения» (Trusted storage subsystem, TSS), и, что более важно, не допускающих хранение критически-важных или конфиденциальных данных вне контроля организации как ответственного хранителя. Данные, которые раскрываются для общественности, обычно размещаются в облачных сервисах, поскольку эти данные легко могут быть заменены без потери контроля над контентом, и тем самым предотвращаются потери верности данных.

Я надеюсь, что вся эта информация поможет всем лучше понять упомянутую исследовательскую статью и проблемы, связанные с принятием решений о том, где размещать критически-важные для миссии организации документы. Хотя эта статья хорошо написана, следует отметить, что большая часть содержащихся в ней сведений устарела и не отражает сегодняшние условия.

Я приветствую дальнейшее обсуждение этой темы, поскольку это очень важный вопрос, который все организации должны принять во внимание до того, как разместят свои критически-важные документы вне своего контроля

как ответственного хранителя, и передадут их под контроль внешней организации или службы.

Эта информация, связанная с защитой критически-важных документов, будет дополнительно обсуждаться на предстоящей конференции IIMC, и в следующей моей статье будут сообщены дополнительные сведения о различных компонентах и соображениях, связанных доверенными документными средами (trustworthy records environments).

Об авторе: Роберт Блатт

Автор данной статьи, Роберт М. Блатт, является основателем консультационной фирмы EID и предоставляет экспертные знания в области «технологий» клиентам EID, которые находятся в процессе «утрамбовывания» своего контента в общекорпоративные электронные системы управления контентом (ECM).

Роберт пользуется большим авторитетом в отрасли управления контентом за многолетнюю работу в американских и международных организациях по стандартизации. Он возглавлял многие усилия по разработке стандартов в ECM-отрасли, в том числе, в последнее время, передовых практик и стандартов, связанных с доверенными ECM-системами, которые дают определение того, что значит иметь доверенную систему управления контентом. Уверенность в том, что то, что Вы получаете из системы именно то, что в неё положили, в конце концов, часто является важнейшей часть головоломки обеспечения управления электронным контентом.

Сопоставьте с высказывания Блатта 2020 года выводы, сделанные в статье Дюранти 2016 года:

«Как будут выглядеть заслуживающие доверия системы обеспечения долговременной сохранности (trustworthy preservation systems) в будущем? Вероятно, они не будут похожи на системы в технологическом смысле этого слова. Скорее, они будут выглядеть как набор взаимосвязанных частей, образующих комплексное целое, стратегическое управление которым, как можно надеяться, будет осуществляться на основе концепции, включающей принципы, правила и процедуры. Это будут гибридные решения - включающие облачные сервисы и собственные сервисы организации; но будут ли они согласованными, интегрированными, взаимозависимыми и интероперабельными, жизнестойкими, высокодоступными и надежными, будет зависеть от будущих технологических разработок и экономических преимуществ.

Доверие к управлению документами и к обеспечению их долговременной сохранности в этих системах будет напрямую связано с надежностью поставщиков услуг и безопасностью облачной архитектуры, инфраструктуры и её операций. Будут ли подобные системы рассматриваться как эффективные решения для управления документами и обеспечения их долговременной сохранности, будет зависеть от способности поставщиков облачных услуг взаимодействовать как по вертикали (когда специализированные поставщики услуг полагаются на более крупных поставщиков), так и по горизонтали, в виде

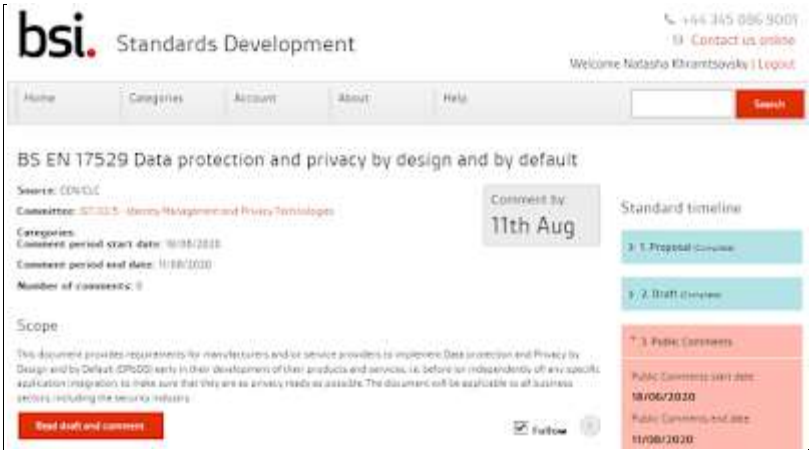
федерации, поддерживающей не только наличие и доступность (availability) посредством избыточности, но и универсальный доступ и все виды обмена информацией. Что касается аутентичности материалов, которые мы будем доверять этим системам, то можно лишь пожелать, чтобы продолжающиеся международные и междисциплинарные исследования смогли обеспечить, чтобы тема аутентичности оставалась в центре внимания».

НОВЫЙ ЕВРОПЕЙСКИЙ СТАНДАРТ EN 17529 «ЗАПРОЕКТИРОВАННАЯ И ПО УМОЛЧАНИЮ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ И НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ»

Источники: сайт BSI / сайт DIN
https://standardsdevelopment.bsigroup.com/projects/2020-00802#/section
https://www.din.de/en/getting-involved/standards-committees/nia/projects/wdc-proj:din21:264709040

Вопросы защиты персональных данных продолжают находиться в центре внимания разработчиков стандартов, и в настоящее время в Европе постепенно подходит к завершению работа над новым стандартом **EN 17529 «Запроектированная и по умолчанию защита персональных данных и неприкосновенности частной жизни»** (Data protection and privacy by design and by default).

На сайте Британского института стандартов можно познакомиться с проектом данного документа и принять участие в его публичном обсуждении, см. https://standardsdevelopment.bsigroup.com/projects/2020-00802#/section



Страница стандарта BS EN 17529 на сайте BSI

Во вводной части документа сказано следующее:

«Настоящий документ предлагает разработчикам компонентов и подсистем формализованный процесс выявления объектов и требований по защите неприкосновенности частной жизни, а также необходимое руководство по проведению соответствующей оценки. Он также помогает понять многоуровневую структуру ответственности и обязательств производителей и поставщиков услуг (с отсылкой к «Общих правилах защиты персональных данных» Евросоюза (General Data Protection Regulation, GDPR, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504) – в частности, к статье 23 (*эта статья ограничивает защиту ПДн, если это требуется в интересах национальной безопасности и т.п. – Н.Х.*), а также к правилам, применимым к приложениям, используемым государственными органами).

В ст. 25 «Общих правил защиты персональных данных» (*которая называется «Запроектированная и по умолчанию защита персональных данных»*) операторам персональных данных и, неявным, производителям вменяется в обязанность внедрить запроектированную и по умолчанию защиту персональных данных. Цель настоящего документа – предоставить производителям и / или поставщикам услуг требования в отношении реализации запроектированной и по умолчанию защиты персональных данных и неприкосновенности частной жизни (Data protection and Privacy by Design and by Default, DPbDD) на ранних стадиях разработки их продуктов и услуг, то есть до (или независимо от) какого-либо конкретного применения или интеграции, - с тем, чтобы убедиться, что они максимально готовы к обеспечению неприкосновенности частной жизни на предполагаемых рынках.

Система менеджмента качества в соответствии с европейским стандартом EN ISO 9001 закладывает основу для процесса создания продуктов и услуг, которые запроектировано включают защиту персональных данных и неприкосновенности частной жизни. Где это необходимо, требования EN ISO 9001 соответствующим образом расширяются. Кроме того, - и в той степени, насколько это применимо на этапе разработки продуктов или услуг, - на основе GDPR сформулированы конкретные цели управления и требования, исполнение которых ожидается от соответствующего поставщика продуктов или услуг. Наконец, описан механизм самодекларирования, который будет применяться, когда это возможно и с учётом разнообразия ожидаемых вариантов использования, в отношении соответствующим образом спроектированных и разработанных продуктов и услуг, помогая тем самым ориентироваться операторам персональных данных, субъектам персональных данных и обществу в целом.

Для некоторых целей обработки и для некоторых категорий персональных данных необходимо провести оценка воздействия на неприкосновенность частной жизни и защиту персональных данных (privacy impact assessment, PIA / data protection impact assessment, DPIA) в соответствии со стандартом EN ISO/IEC 29134 «Информационные технологии - Методы и

средства обеспечения безопасности – Руководство по оценке воздействия на неприкосновенность частной жизни» (Information technology - Security techniques - Guidelines for privacy impact assessment), и в дополнение к требованиям, приведенным в настоящем документе. Необходимо также привести в исполнение следующий из такой оценки план обработки рисков для неприкосновенности частной жизни.

Настоящий документ предназначен для использования производителями, поставщиками, разработчиками аппаратного и программного обеспечения, системными интеграторами, предоставляющими продукты и услуги для использования операторами персональных данных; а также для использования операторами персональных данных при выборе продуктов и услуг для обработки данных.

Содержание документа следующее:

Европейское введение

Введение

1. Область применения

2. Нормативные ссылки

3. Термины, определения и сокращения

4. Общие положения

5. Процесс разработки продуктов и услуг с учётом требований по защите персональных данных (privacy aware)

6. Базовые требования к проектированию продуктов и услуг

7. Требования к самодекларированию того, что при проектировании были учтены требования к защите персональных данных.

ЗМІСТ