ПЕРЕДМОВА

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

У публікації «Внутри арктического хранилища, защищающего человеческую культуру от апокалипсиса» розповідається про використання фотоплівки для збереження найцінніших активів людства.

У публікації «Четыре неправды, уничтожающие управление документами» розповідається що ефективне управління документами єдиний засіб дієвого контролю над світовими інституціями.

У публікації «Сохранение знаний: Как вести себя с уходящими сотрудниками» розповідається про засоби впливу роботи з співробітниками на ефективну роботу установи.

У публікації «Национальные Архивы США: Продолжаем выполнять нашу миссию» розповідається про діяльність архівів США в умовах пандемії Covid-19.

У публікації «Какие документы мы должны хранить на бумаге? Глобальное руководство по соблюдению требований к носителям информации, местонахождению и передаче документов» розповідається про відмінності законодавств країн світу у питаннях збереження документів на папері.

У публікації «Карл Мелроуз: Мы не можем сначала сказать деловым подразделениям, что они - хранители своих документов, а затем - что это не их документы» розповідається про особливості збереження документів.

У публікації «Карл Мелроуз: Практика управления документами без физического контроля над ними, подтверждаемая фактами» розповідається про особливості управління документами за відсутності фізичного контролю.

У публікації «Карл Мелроуз: Ядовитые вопросы» наведено можливі критерії оцінки важливості документів та розподілу зусиль на їх опрацювання.

У публікації «Карл Мелроуз: Почему мы говорим об управлении информацией как активом, если она по большей части таковым не является?» розповідається про особливості та важливість управління інформацією.

У публікації «Международный совет архивов проводит 7-11 июня Международную неделю архивов 2021 года с темой «Расширение возможностей архивов»» розповідається про запланований на червень місяць 2021 року Міжнародний тиждень архівів.

ВНУТРИ АРКТИЧЕСКОГО ХРАНИЛИЩА, ЗАЩИЩАЮЩЕГО ЧЕЛОВЕЧЕСКУЮ КУЛЬТУРУ ОТ АПОКАЛИПСИСА

Источник: сайт Freethink https://www.freethink.com/videos/arctic-world-archive Автор: Дуг Дайс

Катастрофоустойчивый Арктический всемирный архив (Arctic World Archive) был создан для защиты человеческой культуры, и теперь его фонды включают 21 терабайт наших самых важных исходных кодов.

5-минутный видеоролик об Арктическом всемирном архиве доступен по адресу https://www.youtube.com/watch?v=WD8pRlEvCsM .

В глубинах выведенной из эксплуатации угольной шахты, в самом северном поселении мира располагается Арктический всемирный архив (Arctic World Archive). Этот бункер, построенный на случай апокалипсиса, предназначен для обеспечения сохранности для будущих поколений в случае глобальной катастрофы как физических, так и цифровых артефактов.

Он выполняет функции хранилища данных, защищая важные элементы человеческой культуры - реликвии искусства, литературы и религии - от неизвестного будущего. Отражая нынешний оцифрованный мир, хранилище теперь также содержит 21 терабайт открытого исходного кода.

Для реализации этого проекта Арктический всемирный архив объединился с платформой GitHub, служащей для размещения программного кода и являющейся крупнейшим в мире хранилищем программного обеспечения. GitHub работает с операционными системами смартфонов, с платформами цифровых платежей, с агентствами по разработке программного обеспечения с открытым исходным кодом и со многими другими заинтересованными сторонами, помогая им управлять своими продуктами и обеспечивать их безопасность.

Многие из этих продуктов мы используем и взаимодействуем с ними каждый день. Код, на котором они основаны, - это невидимый компонент современной культуры, который стал неотъемлемой частью нашего образа жизни. GitHub выполняет резервное копирование всего этого кода в центрах обработки данных по всему миру, но и жёсткие диски не являются неуязвимыми в случае глобальных катастроф. По этой причине GitHub и Арктический всемирный архив взаимно стремились найти более долгосрочное решение задачи обеспечения сохранности данных – и выбрали в качестве такого решения **фотоплёнку**.

Защищая самые ценные активы человечества

Арктический всемирный архив (о нём см. https://arcticworldarchive.org/about/) был открыт в марте 2017 года, с целью обеспечивать долговременную сохранность наиболее ценных мировых

активов. Хранилище, построенное норвежской компанией по хранению данных Piql, располагается на острове Шпицберген.

Арктический всемирный архив - не первый проект такого рода. На самом деле он находится недалеко от «Глобальное хранилище семян на острове Свальбард» (Svalbard Global Seed Vault, https://www.freethink.com/articles/seed-vault), которое открылось в 2008 году в результате международного соглашения, направленного на сохранение генетического материала растений. Удаленное расположение хранилища семян оказалось идеальным местом и для начала деятельности Арктического всемирного архива.

Сейчас архив находится на глубине 300 метров внутри недействующей угольной шахты в арктических горах. Здесь хранятся рукописи из библиотеки Ватикана, артефакты истории бразильского футбола, шедевры Рембрандта и Мунка и другие культурные ценности, такие, как популярная музыка, научные открытия и политическая история.

В хранилище находятся переданные на депозитарное хранение материалы, поступившие от организаций из 17 разных стран, причём первые депозиты были сделаны национальными архивами Мексики и Бразилии. В 2019 году GitHub в качестве первого этапа работ добавил в хранилище материалы тысяч проектов, включая исходный код операционной системы Android и криптовалюты Биткойн.

Образец записи на плёнке Piql

В этом году GitHub разместил в архиве 21 терабайт открытого исходного кода, уместив всё это на 186 рулонах плёнки Piql - «светочувствительной пленки высокого разрешения, специально разработанной для обеспечения долговечности и высокой плотности записи цифровых материалов».

21 терабайт открытого исходного кода записан на плёнке

Чтобы обеспечить безопасность исходного кода, необходимо было найти автономный носитель, способный противостоять всем мыслимым

угрозам. Как оказалось, химически устойчивая, не позволяющая вносить изменения плёнка является лучшим инструментом для этой цели.

Процесс сохранения данных на плёнке был разработан компанией Piql. Он заключается в преобразовании файлов в QR-коды и последующей записи QR-кодов на отдельные кадры катушечной плёнки. Затем катушка плёнки обрабатывается проявителем, после чего проходит тщательную проверку качества.

«Мы превратили плёнку в современный цифровой носитель информации», - объясняет основатель компании Piql Руне Бьеркестранд (Rune Bjerkestrand). «Вы не можете увидеть это невооруженным глазом, но если Вы поместите плёнку под микроскоп, то увидите отдельные пиксели, заполняющие QR-код сверхвысокого разрешения».

Первые несколько кадров каждой из катушек плёнки содержат инструкции на пяти различных языках о том, как преобразовать QR-коды в пригодные для использования файлы. Все, что понадобится человеку будущего для восстановления данных, - это компьютер, фотокамера и источник света. Катушки с плёнкой хранятся глубоко под землей в контейнерах со стальными стенками.

Передача платформой GitHub своих материалов на депозитарное хранение в Арктический всемирный архив гарантирует, что в случае глобальной катастрофы людям не придётся начинать всё с самого начала, и они смогут воспользоваться сведениями, извлечёнными из этого огромного хранилища материалов внутренней деятельности современного общества.

Считается, что в высокозащищённом хранилище, способном противостоять всему, с чем человечество может столкнуться в ближайшие годы, включая последствия изменения климата - плёнка может сохраняться в течение срока до 500 лет. При этом хранилище также находится в одном из самых геополитически стабильных районов планеты.

Материалы, хранимые арктическим архивом, являются отражением нашего общества – ошибок и подвигов, которые мы совершили. Это символ прогресса и возможностей человечества. И недавнее добавление в архив 21 терабайта кода столь же важно для представления человеческой культуры, как и физические артефакты, которые её сопровождают.

Подобные хранилища крайне важны для человечества в целом. Не нужно, однако, слепо верить оптимистичным обещаниям и делать ставку только на них – так, арктические хранилища уже сообщали о серьёзных неприятностях, связанных с «неожиданным» потеплением климата в районе их расположения (а надеяться, что таких явлений не будет на интервалах времени в многие сотни лет, по меньшей мере, наивно – и, скажем, шведские коллеги, занимающиеся захоронением радиоактивных отходов в том же регионе, учитывают в своих планах возможность новых ледниковых периодов, землетрясений и т.п. катастроф).

Фотоплёнка в идеальных условиях действительно потенциально может благополучно пережить сотни лет, но практический опыт ограничен пока что всего одним столетием (и то с не самыми лучшими результатами); и уже

были случаи, когда в очень хорошо оборудованных хранилищах по каким-то причинам хранимая в стальных контейнерах плёнка начала разрушаться, что выяснилось лишь тогда, когда после сильных наводнений в Германии потребовались резервные копии документов и контейнеры были вскрыты.

Как альтернатива может рассматриваться идеология ряда британских цифровых архивистов: согласно которой первостепенная задача - сохранить цифровые материалы в течение 30-40 лет и передать их в приличном, пригодном для использования состоянии, следующему поколению, которое примет у нас эстафету.

ЧЕТЫРЕ НЕПРАВДЫ, УНИЧТОЖАЮЩИЕ УПРАВЛЕНИЕ ДОКУМЕНТАМИ

Источник: блог «Управление документами следующего поколения» (Next Generation Records Management) https://nextgenrm.com/2021/02/10/the-four-lies-destroying-records-management-lie-1-information-vs-data/

Автор: Дон Людерс

Эффективное управление документами, осуществляемое добросовестно, является единственным средством для привлечения наших самых могущественных институтов к ответственности за их поведение, - и эти же самые институты в течение почти двух десятилетий ведут жестокую войну с профессией управления документами.

К сожалению, они побеждают в этой войне, о чем свидетельствует бурный информационный хаос, охвативший все частные и государственные организации по всему миру. Трагические последствия этого безудержного информационного хаоса - политические потрясения, финансовое разорение, гибель ни в чем не повинных людей – это тот вид зла, который традиционно практиковался лишь наиболее репрессивным и тираническим режимам в истории, но теперь заразил ряд наиболее развитых обществ в мире.

Всякое злое поведение построено на лжи, и война с управлением документами не исключение. Могущественные силы, полные решимости уничтожить нашу древнюю и благородную профессию, хотят, чтобы Вы поверили в четыре ключевые неправды, с тем, чтобы они могли избежать подотчётности и помешать прозрачности и информационной безопасности, которые обеспечивает управление документами.

Данный пост является первым в серии статей, в которых объясняются эти четыре лжи и их разрушительное влияние на эффективное управление документами.

Ложь №1: «Данные и информация – одно и то же»

Данные представляют собой набор значений. Это гигантское «ведро», наполненное буквами, цифрами и символами. Сами по себе данные бесполезны.

Такая трактовка термина «данные» соответствует терминологии Международной организации по стандартизации (ИСО), согласно которой данные – это, по сути, пригодные для машинной обработки некие коды, рассматриваемые вне какого-либо контекста, интерпретации и т.д. Согласно ИСО, именно осмысленность и интерпретация превращают данные в информацию. Следует, однако, иметь в виду, что такая точка зрения – не единственная, и многие специалисты понимают данные как информацию, представленную в удобной для обработки форме.

Похоже, сотрудники компании Paycom это понимают. Вот скриншот из отличного рекламного ролика, который они недавно распространяли:

Эти бедные люди на снимке буквально по пояс погрязли в «данных» - которые представляют собой просто болото из бессмысленных, неконтролируемых значений, замедляющее их работу и делающее несчастной их жизнь.

Любая организация может создать огромное количество бесполезных данных. Но если вы поместите эти данные в контекст, они станут «информацией» - и это придаст им ценность.

Речь идёт о 29-страничном документе «Белая книга по когнитивным технологиям – Последствия для управления документами интернета вещей, роботехнической автоматизации технологических процессов и производств, машинного обучения и искусственного интеллекта» (Cognitive Technologies White Paper - Records Management Implications for Internet of Things, Robotic Process Automation, Machine Learning, and Artificial Intelligence), см. https://www.archives.gov/files/records-mgmt/policy/nara-cognitive-technologies-whitepaper.pdf .

Компания Paycom хочет, чтобы Вы заплатили им за это: Влейте свои бесполезные данные в их решение, чтобы Вы могли использовать их для создания информации:

Очевидно, что «данные» и «информация» - это две взаимосвязанные, но разные вещи. Но если это так, то почему такая могущественная организация, как федеральное правительство США, похоже, этого не понимает? И почему Национальные Архивы США говорят в своём опубликованном в октябре 2020 года аналитическом отчёте по когнитивным технологиям следующее:

«Управление данными с точки зрения применения методов и дисциплины управления документами, закреплено в разделе 44 U.S.C. 33 Свода законов США, в статье 3301, в которой говорится, что понятие «федеральные документы» «охватывает любую документированную информацию, независимо от её формы и характеристик». Термин «данные» в соответствии с определением, приведенным в ст. 3502 главы раздела 44 U.S.C. 35 Свода законов США, означает «зафиксированную (задокументированную) информацию независимо от её формы».

Определение понятия «данные» в 44 USC 3502 (16) (см. https://www.law.cornell.edu/uscode/text/44/3502 *) полностью звучит так: «Термин «данные» означает зафиксированную информацию, вне зависимости от её формы и от носителя информации, на котором данные записаны».*

Думаете, смешение понятий «данные» и «информация» не вызывает проблем? Тогда подумайте вот о чём. Во всех органах исполнительной власти федерального правительства США есть должностное лицо, ответственное за управление документами этого органа (Agency Records Manager). Он или она отвечает за программу управления жизненным циклом документов соответствующего органа. По определению, понятие «документы» охватывает «всю документированную (*или зафиксированную – recorded*) информацию», поэтому ведомственная программа управления документами отвечает за управление информацией этого ведомства.

Теперь, однако, благодаря Закону об «открытых, публичных, электронных и необходимых государственных данных» (OPEN Government Data Act), в каждом органе исполнительной власти назначается директор по данным (Chief Data Officer), которому поручено возглавить новую огромную внутреннюю бюрократию, «отвечающую за управление данными на протяжении их жизненного цикла».

Если понятие «данные» трактуется федеральным правительством США как «зафиксированная информация», то каким образом обязанности директора по данным (Chief Data Officer) за управление жизненным циклом данных могут напрямую не перекрываться с обязанностями ответственного за управление документами ведомства (Agency Records Manager) за управление жизненным циклом документов?

Правда заключается в том, что благодаря смешению понятий «данные» и «информация» обязанности ответственного за управление документами и директора по данным федерального органа исполнительной власти оказываются ***совершенно одинаковыми***, и каждый такой орган в составе федерального правительства теперь имеет ***две*** бюрократические структуры, отвечающие за управление жизненным циклом государственной информации. Подобное перекрытие приводит к внутренним конфликтам в государственных органах, что делает прогресс в управлении жизненным циклом ***любой*** информации этих органов практически невозможным.

На практике ситуация обычно не столь трагична. Часто специалисты по управлению документами преимущественно занимаются управлением информацией с учётом её содержания, а также её правовой, деловой и иной ценности, в то время, как специалисты по управлению данными уделяют основное внимание вопросам управления соответствующей инфраструктурой и компетенциями – абстрагируясь от содержания и ценности информации.

Всё это также существенно подрывает эффективность и репутацию программы управления документами федерального органа исполнительной власти… что, возможно, всегда и было главной задачей.

Ложь №2: «Обеспечение долговременной сохранности и хранение одно и то же»

В течение нескольких месяцев после президентских выборов некоторые из ведущих СМИ, в том числе служба телевещания PBS и журнал New Yorker Magazine, публиковали статьи, настойчиво напоминающие администрации Трампа об её обязанности, в соответствии с Законом о президентских документах (Presidential Records Act), «предпринять все необходимые шаги для обеспечения того, чтобы деятельность, обсуждения, решения и политики, которые отражают выполнение Президентом установленных Конституцией и законодательством, а также иных официальных или церемониальных обязанностей, были должным образом документированы, и чтобы была обеспечена ***долговременная сохранность*** таких документов и их хранение в качестве президентских документов».

На рис. мальчик говорит: «Если нечто может быть уничтожено правдой, оно заслуживает того, чтобы быть уничтоженным правдой»

Я не ставлю под сомнение мотивы этих публикаций. Я уверен, что их авторы хотят, чтобы Белый дом Трампа столь же строго был подотчётен за свои действия, как и предыдущие президентские администрации были подотчётны за их действия. Но я действительно сомневаюсь, понимают ли авторы этих публикаций, чего именно они требуют … и способен ли это вообще обеспечить любой из обитателей Белого дома.

Федеральные документы определяются как «любая документированная информация». ***Хранить*** документы (то есть информацию) просто. Однако ***обеспечить долговременную сохранность*** информации намного сложнее. Это связано с тем, что хранение и обеспечение долговременной сохранности - две разные вещи.

Если я кладу стейк на косточке в холодильник - где он легкодоступен, но при этом также может легко испортиться, - это ***хранение***. Если я положу этот же стейк в морозильную камеру - где он несколько менее доступен, но при этом более защищен от порчи в течение гораздо более длительного периода времени, - это ***обеспечение долговременной сохранности***.

Точно так же, если я держу бумажный документ в ящике письменного стола, - я его ***храню***. Но если я приношу тот же самый бумажный документ в центр хранения документации моей компании и прошу руководителя корпоративной службы управления документами провести его классификацию, упаковать и положить на полку до истечения соответствующего срока хранения, я ***обеспечиваю его долговременную сохранность***.

Хранение и обеспечение сохранности электронной информации точно так же различаются. Я могу хранить электронные документы где угодно: на общих дисках, на USB-накопителях, в ноутбуках, и даже в памяти принтера (см. https://www.komando.com/tech-tips/dont-sell-your-printer-before-doing-this-1-critical-step/331796/). Но если я хочу обеспечить его долговременную сохранность, мой список вариантов становится намного короче.

Пункт 36 CFR §1236.20 Свода федеральных нормативных актов США (см. https://www.law.cornell.edu/cfr/text/36/1236.20) описывает «надлежащие системы управления документами» (appropriate records keeping systems) для

электронных документов федерального органа исполнительной власти (и для Белого дома). В нём, в частности, сказано, что эти системы должны «предотвращать несанкционированный доступ, модификацию или удаление зарегистрированных документов, и обеспечивать наличие надлежащих журналов аудита для отслеживания использования этих документов». Также требуется, чтобы эти системы «…поддерживали миграцию документов и связанных с ними метаданных на новые носители информации и/или в новые форматы во избежание утрат из-за деградации носителей информации или устаревания технологий». Иными словами, эти системы должны быть способны ***обеспечивать долговременную сохранность*** документов, а не просто ***хранить*** их.

Но сохранялись ли документы администрации Трампа в системах управления документами, соответствующих требованиям п. 36 CFR §1236.20? Я не могу с уверенностью ответить на этот вопрос. Я не занимался управлением президентскими документами со времён последней администрации Буша. Но, основываясь на моём почти четвертивековом опыте поддержки управления федеральными документами, я могу сказать Вам, что это весьма маловероятно (см. https://www.theepochtimes.com/the-illusion-of-transparency_3234958.html).

Итак, если предположить, что некоторые - возможно, все - электронные документы администрации Трампа скорее ***хранились***, чем ***обеспечивалась их сохранность***, то что это значит для историков и журналистов? Что это означает для членов администрации Трампа, включая самого президента? И, самое главное, что это значит для американской общественности?

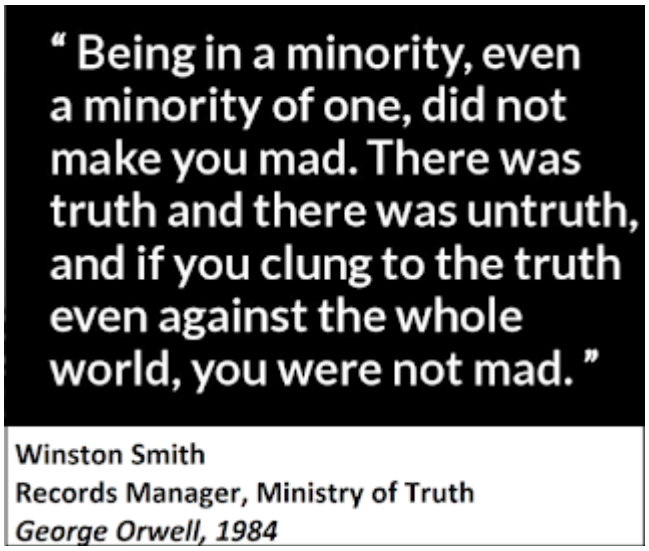
К сожалению, это плохо для всех. Журналисты и историки, пишущие о периоде президентства Трампа, должны быть уверены в том, что информация, которую они получают в соответствии с запросами на основе законодательства о свободе доступа к государственной информации (FOIA), является аутентичной, и что никакие электронные документы не были несанкционированно изменены или уничтожены. Члены администрации Трампа должны иметь возможность доказать то же самое. И американский народ, как всегда, заслуживает того, чтобы знать правду, какой бы она ни была. К сожалению, если администрация Трампа скорее ***хранила*** свои документы, чем ***обеспечивала их долговременную сохранность***, всё это может оказаться невозможным.

Могущественным силам, стремящимся уничтожить управление документами, нужно, чтобы Вы поверили, что хранение информации - в их дорогостоящих хранилищах, на их огромных платформах для коллективной работы, в их гигантских облачных средах - это то же самое, что и обеспечение долговременной сохранности информации. Но это не так. И пока это не будет широко осознано, и обеспечение долговременной сохранности документов не станет требованием для всех организаций, - как государственных, так и частных, - мир будет продолжать тонуть в неточной информации, дезинформации и лжи.

Ложь №3: «Обеспечение безопасности и доступа – одно и то же».

Спустя несколько недель после обнаружения утечки данных вследствие кибератаки типа Sunburst (*речь идёт о нашумевшей атаке на клиентов известной компании SolarWinds, действующей в сфере обеспечения информационной безопасности*), новостное агентство BBC взяло интервью у Брайана Лорда (Brian Lord), бывший заместитель директора по кибероперациям британского разведывательного ведомства GCHQ (о нём см. https://ru.wikipedia.org/wiki/Центр_правительственной_связи - *это спецслужба, ответственная за ведение радиоэлектронной разведки и обеспечение защиты информации органов правительства и армии Великобритании*).

Г-н Лорд согласился с тем, что результатом кибератаки, которая привела к компрометации информационных систем ряда федеральных органов исполнительной власти США, в том числе министерств финансов, иностранных дел, национальной безопасности и энергетики, - была разрушительная утрата государственной информации. В то же время он отметил: «Я думаю, будет справедливо сказать, что дополнительные уровни безопасности вокруг документов высшей и высокой степени секретности останутся в неприкосновенности благодаря внутренним мерам контроля и управления, поэтому прямой доступ к этим материалам маловероятен».



На рис. приведена цитата: «Будучи в меньшинстве, даже оставаясь один против всех, вы не безумны. Была правда и была ложь, и если вы отстаиваете правду даже против всего мира, вы не безумец» - это слова Уинстона Смита (Winston Smith), специалиста по управлению документами в Министерстве правды – главного героя знаменитого романа Джорджа Оруэлла (George Orwell) «1984».

Какие внутренние меры и средства контроля и управления доступом имел в виду г-н Лорд? Кто отвечает за эти меры и средства контроля доступа? И, что наиболее важно, что случилось бы с чувствительными и

секретными федеральными документами, если бы эти меры и средства управления доступом никогда не были реализованы?

Когда дело доходит до управления жизненным циклом информации (а эту работу специалисты по управлению документами выполняют в течение тысячелетий), «безопасность» и «доступ» - это две очень разные вещи.

Не так давно, в те дни, когда документированная информация хранилась почти исключительно на бумаге, обеспечение ***безопасности*** заключалось в заборе, колючей проволоке, видеокамерах и решетчатых окнах центра хранения документации компании. Управление ***доступом*** выражалось в том, что специалист по управлению корпоративными документами проверял, есть ли у желающего просмотреть документ компании человека разрешение на это.

Сохраняемая в электронном виде информация ничем в этом смысле не отличается. Для типичной корпоративной ИТ-системы можно привести длинный список как аппаратных, так и программных решений, используемых для обеспечения безопасности её сетей. Брандмауэры, антивирусная защита, белые и черные списки, решения для сегментации сети, инструменты шифрования… Этот список практически бесконечен.

Но, как снова и снова демонстрируют последние новости, пока что никакая комбинация этих решений по обеспечению безопасности не доказала свою способность помешать решительно настроенным и хорошо финансируемым злоумышленникам получить доступ к некоторым из самых защищённых сетей в мире. Именно в такой ситуации меры и средства управления доступом, за которые несут ответственность специалисты организации по управлению документами, играют ключевую по важности роль в смягчении ущерба, связанного со взломом и утечкой данных.

В течение последней четверти века практически все «приложения для управления документами»', проданные федеральным органам исполнительной власти США, были смоделированы (и сертифицированы) на основе стандарта DoD 5015.2 «Требования к проектированию электронных систем управления документами» (Electronic Records Management Software Applications Design Criteria, см. также пост https://community.aiim.org/blogs/don-lueders%20crm%20cdia/2013/05/27/on-why-i-no-longer-support-the-dod-5015.2-standard). Фактически, решения, сертифицированные на соответствие DoD 5015.2, являются единственными приложениями, специально упомянутыми в федеральном нормативном акте, описывающем адекватные системы для управления электронными документами государственных органов – это раздел 36 CFR 1236.20 Свода нормативных актов США (см. https://www.law.cornell.edu/cfr/text/36/1236.20).

Вот как стандарт DoD 5015.2 определяет понятие «управление доступом»:

DL1.2. Access Control. The term "access control" has the following meanings:

DL1.2.1. A service feature or technique used to permit or deny use of the components of a communication system.

DL1.2.2. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device.

DL1.2.3. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. Types of access control methods include Mandatory Access Control and Discretionary Access Control (Reference (c)).

DL1.2.4. The process of limiting access to the resources of an AIS to authorized users, programs, processes, or other systems. (DL1.15)

DL1.2.5. The function performed by the resource controller that allocates system resources to satisfy user requests.

DL1.2. Управление доступом (Access Control). Термин «управление доступом» имеет следующие значения:

DL1.2.1. Функциональная возможность сервиса или метод, который используется для разрешения или запрещения использования компонентов коммуникационной системы.

DL1.2.2. Метод, используемый для предоставления или ограничения прав физических лиц или прикладных программ на получение данных с запоминающего устройства или на размещение данных в нём.

DL1.2.3. Предоставление или ограничение прав физических лиц или прикладных программ на получение данных с запоминающего устройства или на размещение данных в нём. Типы методов контроля и управления доступом включают мандатный контроль доступа (Mandatory Access Control - *т.е. в строгом соответствии с полномочиями или правилами*) и дискреционный контроль доступа (Discretionary Access Control – *когда сетевые администраторы избирательно, на своё усмотрение, предоставляют некоторым пользователям доступ к ресурсам*, ссылка (c)).

DL1.2.4. Процесс ограничения доступа к ресурсам автоматизированных информационных систем (Automated Information Systems, AIS), который разрешается только авторизованным пользователям, программам, процессам или другим системам. (DL1.15)

DL1.2.5. Функция, выполняемая контроллером ресурсов (resource controller), который выделяет системные ресурсы для удовлетворения запросов пользователей.

Стандарт содержит множество требований к реализации мер и средств контроля и управления доступом в сертифицированном хранилище документов. В качестве примера приведём тестовую матрицу управления доступом, используемую Агентством оборонных информационных систем (Defense Information Systems Agency, DISA) в рамках базовой проверки систем на соответствие DoD 5015.2:

Table 2-1.1. Verify Users							
Full Name	User ID	Password	Clearance Level	Project Name Access	Supplemental Markings Assigned	Set Up In	
						OS	RMA
Rangel, Jan	rangelj	rrrRRRIII111rrr	TOP SECRET	Project A Project B Project C	OMIKRON NATO THORS HAMMER FRD RD		
Martinez, Dan	martinezd	mmmMMMIII111mmm	TOP SECRET	Project A Project B Project C	OMIKRON NATO THORS HAMMER FRD RD		
Rogers, Josh	rogersj	rrrRRRIII111rrr	SECRET	Project A Project B	NATO THORS HAMMER FRD RD		
Franco, Dustin	francod	fffFFFIII111fff	SECRET	Project A Project C	OMIKRON NATO THORS HAMMER FRD RD		
Smith, Guido	smithg	sssSSSIII111sss	CONFIDENTIAL	Project A	NATO THORS HAMMER FRD RD		
Ly, Ann	lya	lllLLLIII111lll	No Clearance	Project A Project C	THORS HAMMER		
Harris, Earl	harrise	hhhHHHIII111hhh	No Clearance	Project C	NATO THORS HAMMER		
Sandy, Diane	sandyd	sssSSSIII111sss	No Clearance	Project C	OMIKRON NATO		
McNeil, Helen	mcneilh	mmmMMMIII111mmm	SECRET		OMIKRON NATO THORS HAMMER		
Bayless, Betsy	baylessb	bbbBBBIII111bbb	CONFIDENTIAL		OMIKRON NATO		

Обратите внимание на то, что в этом тестовом примере права пользователей определяются тремя категориями управления ***доступом***: это **«Уровень допуска»** (Clearance Level); настраиваемая категория на основе метаданных (в данном примере, на основе определяемого пользователем поля под названием **«Имя проекта»** (Project Name)); и категория **«Дополнительные грифы»** (Supplemental Markings). Для прохождения базовой сертификации требуется реализовать все эти три различные формы контроля и управления доступом.

В сертифицированном на соответствие DoD 5015.2 решении специалист по управлению документами может применять эти меры контроля и управления, в бесконечной комбинации, к отдельным документам, группам документов, папкам и подпапкам в рамках всей классификационной схемы хранилища документов. И если злоумышленник взломает систему информационной безопасности организации, то эти средства контроля и управления не позволят ему получить доступ ко всей информации в хранилище. Это и есть те «меры и средства внутреннего контроля», которые г-н Лорд имел в виду, когда его спросили об утечках данных в результате Sunburst-атаки.

Но что если ни один федеральный орган исполнительной власти (включая Национальные Архивы США!) никогда на самом деле не вводил сертифицированное по DoD 5015.2 решение в производственную эксплуатацию, - о чём подробно рассказано в статье, опубликованной (см. https://www.theepochtimes.com/the-illusion-of-transparency_3234958.html) в номере журнала Epoch Times за февраль 2020 года?

К сожалению, это означало бы, что ни одна из этих критически важных мер и средств контроля и управления доступом никогда бы не применялся в отношении какой-либо документированной информации государственного органа, и что любой, кто обошёл систему сетевой безопасности этого органа, мог бы свободно путешествовать по ведомственным документальным источникам, похищая, изменяя или уничтожая информацию по своему желанию.

Это также означало бы, что взлом Департамента по управлению персоналом органов федерального правительства США (Office of Personnel Management, OPM) в 2015 году (о нём см. https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach), Sunburst-кибератаки, а теперь ещё и кража электронной переписки из серверов Microsoft Exchange (https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/) спонсируемыми государством китайскими хакерами являются в колоссальной степени более разрушительными, чем готов признать кто-либо в технологической индустрии или в правительстве США.

Враги управления документами хотят, чтобы Вы поверили, что «безопасность» и «доступ» - это одно и то же, потому что они жаждут неограниченного контроля над самым ценным товаром в мире - информацией. До тех пор, пока меры и средства контроля и управления доступом, за которые отвечает служба управления документами организации, не станут последовательно применяться к документам в масштабах всей организации, сама критически-важная в мире информация будет находиться на ужасающем уровне уязвимости, и эти разрушительные взломы и атаки будут продолжаться.

Ложь №4: «Документы и не-документы сильно отличаются друг от друга».

Много лет назад, когда я еще только начал заниматься управлением записями, и я изо всех сил пытался сформировать свое собственное понимание жизненного цикла информации, я работал в качестве консультанта и технического представителя продаж для небольшого поставщика программного обеспечения, который создал и продал "предприятие записи управления приложением. Основная часть нашей клиентской базы были федеральные правительственные учреждения США, и я послушно следовал документированной философии правительства, что некоторые части записанной информации могут быть классифицированы как "записи", в то время как некоторые другие части записанной информации могут быть классифицированы как "не-записи".

Когда я хотел бы продемонстрировать электронную почту записи управления функциональностью нашего приложения, я часто использую приглашение по электронной почте на обед в качестве примера "не-записи", которые не требуют сохранения в нашем решении на основе федеральных правил управления записями. Со временем электронная почта "Let's Go to

Lunch" стала своего рода отраслевым стандартом для понимания концепции того, какой тип информации федерального агентства представляет собой "не-запись".

Но, когда я начал интересоваться, чтобы узнать больше о дисциплине управления записями, меня стало все больше *беспокоить* понятие любой записанной информации "не-запись". Маркировка чего-то не-записи означает, что информация не имеет ценности и не достойна строгих бизнес-правил, необходимых для эффективного управления жизненным циклом информации. Но вся информация записывается по причине, и кто-то должен сказать, что часть какой-либо одной информации не является ценной в любой момент времени?

Возьмем в качестве примера электронную почту "Let's Go to Lunch". Конечно, это звучит бессмысленно на первый взгляд, но что, если приглашение было отправлено мужчиной вице-президентом Корпорации одной из своих подчиненных-женщин? А что, если это было *двадцатое* письмо, которое он послал ей за последние несколько месяцев с просьбой пойти пообедать? А что, если подчиненный в конце концов подаст иск, утверждая, долгую историю сексуальных домогательств со стороны вице-президента? Не будет ли эта "не-запись" электронной почты иметь огромное значение для этой женщины, и не должна ли она быть сохранена в течение некоторого общепринятого периода времени?

С юридической точки зрения, называете ли вы часть записанной информации "запись" или "не-запись" не имеет смысла, потому что это *всегда доказательства,* и *это всегда проявляется* в гражданском вопросе. Но те люди, которые стремятся уничтожить управление записями, хотят, чтобы вы поверили, что маркировка информации как «не-записи» освобождает их от ответственности за сохранение и управление этой информацией. Таким образом, они могут защитить себя от судебного преследования, когда потенциальные доказательства их неправильного поведения "потеряли" или "удалены", утверждая, что это была "не-запись", и поэтому они не сделали ничего плохого, не сохраняя ее.

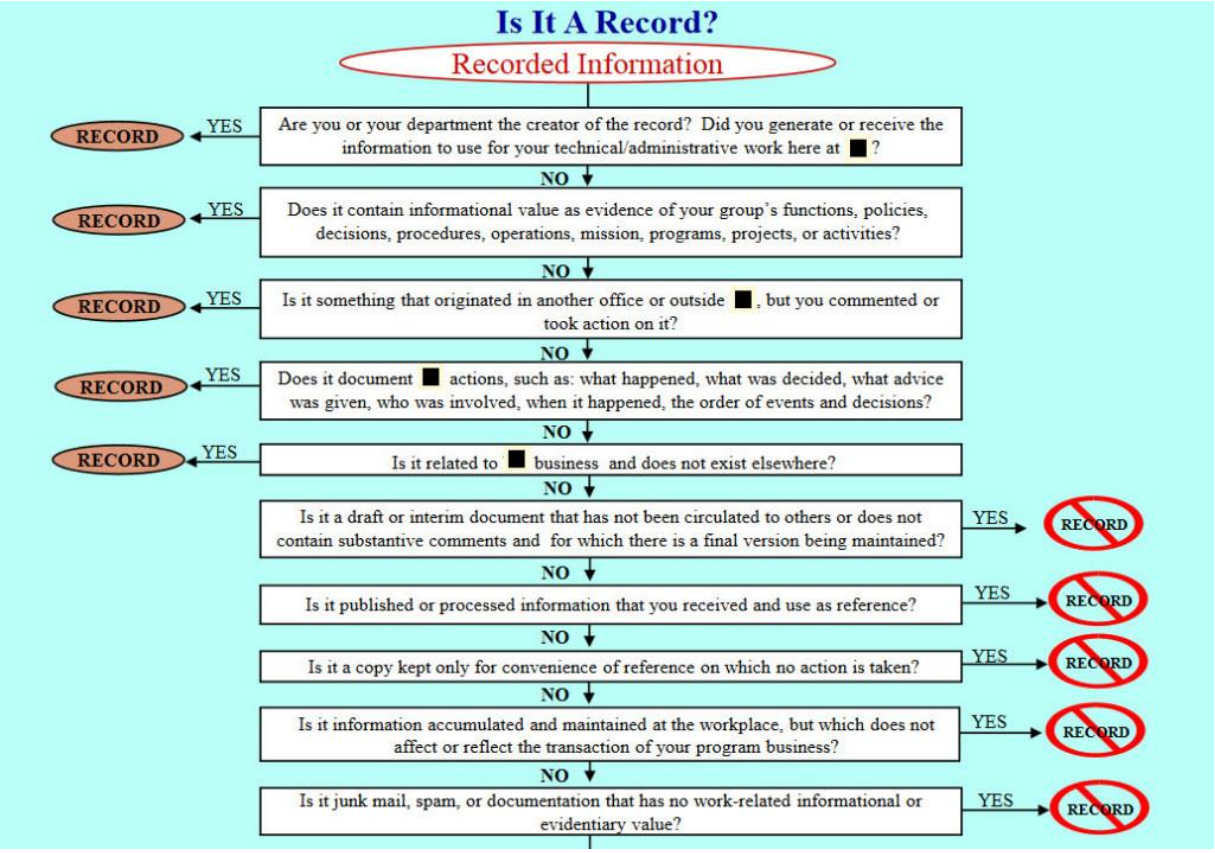
Как я уже отмечал в предыдущем посте, федеральное правительство определяет "запись" как "все записанные сведения". Это была небольшая модификация определения, сделанного в 2014 году, которая имела глубокие последствия для управления записями федеральных агентств.

Как теперь можно продолжать разделять информацию федерального агентства на "записи" и "не-записи" на основе этого нового определения? Правда в том, что ты этого не можешь. Однако, к сожалению, во многих учреждениях (и слишком многих организациях частного сектора) эта практика сохраняется. Эта политика должна прекратиться, если какая-либо организация когда-либо будет в состоянии эффективно управлять своей записанной информацией.

Но, возможно, удивительно, что это на самом деле хорошая новость для менеджеров по записям. Это связано с тем, что управление *жизненным* циклом всей записанной информации организации является более

безопасным, более эффективным и менее дорогостоящим, чем разделение этой информации на "записи", которые должны управляться, и "не-записи", которые должны быть проигнорированы.

Это верно для длинного списка причин. Вот один. Это дерево решений, используемое в течение многих лет в нескольких федеральных агентствах, которое призвано помочь информационному работнику агентства определить, является ли определенная часть записанной информации "записью" или "не-записью" (мной сделанны редакции, для того чтобы предотвратить идентификацию какого-либо одного учреждения):



Удивительно, но сотрудники агентства информации были обучены передавать *каждую часть записанной информации, которую* они создали или получили через этот сложный рабочий процесс, просто чтобы определить, если информация была "запись" или "не-запись". Это включало электронные письма, мгновенные сообщения, текстовые сообщения, неструктурированный контент, даже голосовую почту.

Подумайте о количестве информации, которую вы генерируете на *вашей* работе. Сколько времени вне вашего дня потребуется вам, чтобы запустить каждый из этих частей информации через этот рабочий процесс? Все это время будет потрачено впустую, учитывая, что нет никакой реальной ценности в маркировке части информации "запись" или "не-запись". Устраните это требование, и информационный работник будет иметь гораздо больше времени, чтобы сделать важную работу, за которую он или онаполучает оплату.

Классификация части записанной информации как «записи» или «не-записи» является одним из многих реликвий бумажной программы управления записями, которая не имеет реальной ценности в цифровой информационной среде. Прекращение этой практики позволило бы значительно улучшить возможности любой организации в области управления жизненным циклом информации и должно быть стандартной политикой во всем мире.

СОХРАНЕНИЕ ЗНАНИЙ: КАК ВЕСТИ СЕБЯ С УХОДЯЩИМИ СОТРУДНИКАМИ

Источник: сайт компании Lucidea https://lucidea.com/blog/knowledge-retention-how-to-deal-with-a-departing-workforce/

За последние 20 лет много было написано о масштабной утечке мозгов, текучести кадров и стареющей рабочей силе. Независимо от того, как это называется, проблема заключается в том, что существенные знания во многих организациях выходят за дверь и больше уже не вернутся. В этом посте обсуждается эта проблема и как её можно решать.

Подразделения теряют опыт и знания по разным причинам, в числе которых:

- **Уход на пенсию:** Сотрудники выходят на пенсию либо из-за возраста, либо из-за неспособности или нежелания найти новую работу;
- **Повышение по службе, перемещение и смена ролей:** Люди уходят со своей работы из-за того, что переходят на новую;
- **Использование временного персонала, подрядчиков и консультантов:** Для выполнения определенных ролей вместо полной занятости начинают использоваться неполный рабочий день или непостоянная занятость, что негативно влияет на преемственность;
- **Слияния, поглощения, консолидации и реорганизации:** Реструктуризация организации приводит к добровольному и вынужденному уходу сотрудников;
- **Изменения в стратегии, направленности или специальности:** Организации выбирают новые направления деятельности и соответственно заменяют персонал;
- **Сокращение штатов:** Меры по сокращению затрат приводят к увольнениям;
- **Менталитет краткосрочной работы:** Постоянные, лояльные сотрудники не ценятся и считаются чудаками, - в то время, как идёт погоня за быстрой прибылью;

- **Разочарование:** Сотрудники, видя бесконечные изменения, массовые увольнения, и неудачи руководства, становятся циничными по отношению к организации;
- **Болезнь, смерть или необходимость ухода за близкими:** Люди заболевают, умирают или вынуждены посвятить себя уходу за родственниками;
- **Уход на новую работу:** Сотрудники находят работу в других организациях.

Пять возможных путей решения данной проблемы:

- **Обмен информацией:** Попросите тех, кто может покинуть организацию, поделиться документами, идеями, находками, советами, приемами и методами;
- **Инновации:** Попросите сотрудников-ветеранов предложить более эффективные способы работы на основе их опыта;
- **Повторное использование:** Институционализируйте процессы для повторного использования извлечённых уроков, проверенных практик и полученных результатов;
- **Сотрудничество:** Создайте условия для сотрудничества между уходящими и остающимися сотрудниками;
- **Обучение:** Прикрепите учеников к опытным наставникам.

Здесь можно применить следующие десять методов управления знаниями:

- **Использование проверенной практики:** Документируйте, копируйте и повторяйте;
- **Извлечённые уроки:** Документируйте, анализируйте и повторно используйте;
- **Создание профессиональных сообществ:** Попросите всех представителей одной специальности, от новичков до специалистов со стажем и пенсионеров, присоединиться и принять участие в их работе;
- **Анализ социальных сетей:** Выявите ключевые «соединительные узды» и авторитетные ресурсы;
- **Корпоративные социальные сети:** Обеспечьте возможность онлайн-общения, материалы которого можно снабжать тегами, сохранять и вести по ним поиск;
- **Видео:** Записывайте учебные материалы, находки и истории, а затем заставляйте других сотрудников их смотреть;
- **Сбор документов:** Добавляйте документы, снабжайте тегами и обеспечьте возможность поиска по ним;
- **Рассказывание историй:** Попросите людей рассказывать истории во время общественных мероприятий, в процессе обучения и в записанных видео;

- **Стимулы:** Предложите стимулы, поощряющие делиться знаниями, повторно использовать их и оставаться на связи после увольнения - особенно в качестве активных членов профессиональных сообществ;
- **Карты знаний (knowledge maps):** Проведите инвентаризацию основных знаний, включая сведения о том, какие знания необходимы, кто ими располагает, как они используются и передаются.

Ниже приведены десять идей относительно того, как сохранять знания организации:

- Убедитесь, что у Вас действует программа управления знаниями. Не ждите до последнего момента, когда люди вот-вот уйдут на пенсию или покинут организацию;
- Сохраняйте в архиве собранные профессиональными сообществами наработки и материалы проведенных дискуссий;
- Попросите своих идеологов разработать учебные курсы по их специальностям;
- Предложите стимулы за подготовку персональных руководств по процессам, контактам и контенту;
- Проведите собеседования с использованием видео и используемых профессиональными сообществами инструментов общения, чтобы собрать истории, инструкции и рекомендации;
- Попросите людей представить десять наиболее часто используемых ими документов;
- Составьте карту знаний с целью определить источники знаний, их потоки и ограничения;
- Как можно раньше до ухода опытных сотрудников сформируйте пары наставник / ученик;
- Проведите семинары по «передаче эстафеты», в ходе которых уходящие сотрудники могли бы поделиться своим опытом и ответить на вопросы;
- Сформируйте сообщество бывших сотрудников организации и дайте возможность пенсионерам продолжать участвовать в деятельности сообществ до тех пор, пока они в силах вносить свой вклад.

НАЦИОНАЛЬНЫЕ АРХИВЫ США: ПРОДОЛЖАЕМ ВЫПОЛНЯТЬ НАШУ МИССИЮ

Источник: блог Архивиста США «AOTUS» https://aotus.blogs.archives.gov/2021/03/01/moving-our-mission-forward/

С начала пандемии коронавируса Covid-19 значительная часть Национальных Архивов США (NARA) работала на 100% дистанционно. Даже несмотря на ограниченность наших возможностей выполнять работу на штатных рабочих места и невероятно сложные обстоятельства, наши сотрудники продолжали демонстрировать свой творческий потенциал, инициативу и приверженность дальнейшему выполнению нашей миссии.

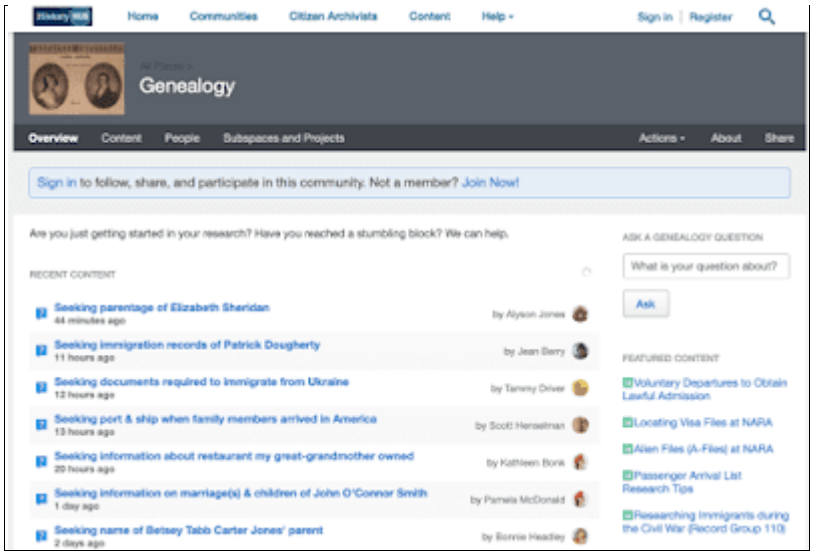
По всей стране сотрудники отдела услуг для исследователей (Office of Research Services) отвечают на запросы; формируют списки коробов и папок, которые помогают исследователям получать доступ к документам и поддерживают выполнение текущих и будущих проектов оцифровки; готовят оцифрованные дела и метаданные и представляют их на загрузку в Каталог Национальных Архивов США; выполняют контроль качества цифровых изображений; пишут посты в блогах; делают ту часть работы по архивной обработке и описанию, которая может выполняться удаленно, и многое другое. Их поразительные усилия позволили нам установить связь с нашими клиентами и обеспечить доступность архивных материалов даже в период глобальной пандемии, - и ниже я хотел бы подробнее рассказать о нескольких проектах.

В Центре изучения истории (History Hub, https://historyhub.history.gov/welcome), - это платформа Национальных Архивов, на которой любой может задавать связанные с историей вопросы и получать ответы от широкого круга различных экспертов, - сотрудники отдела услуг для исследователей модерируют поступающие вопросы и координируют подготовку ответов Национальными Архивами, часто с привлечением нескольких сотрудников - например, ответ на вот этот (см. https://historyhub.history.gov/thread/8776) вопрос о том, когда органы правительства США перешли с рукописей на машинописные документы.

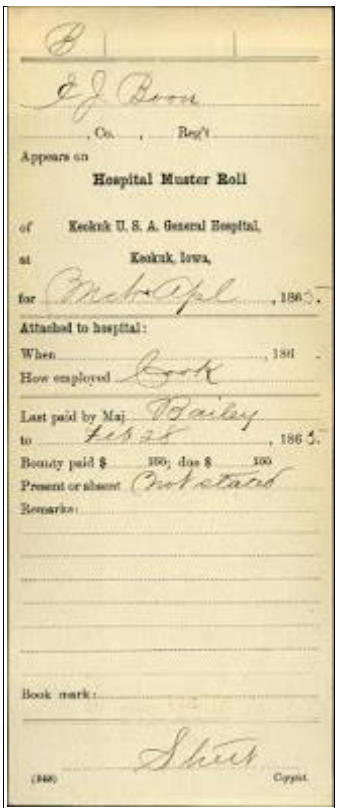
Кроме того, сотрудники этого отдела публикуют мнения экспертов и полезную информацию по широкому кругу тем, начиная от «Поиска дел о выдаче виз в Национальных Архивах» (см. https://historyhub.history.gov/community/genealogy/blog/2020/07/06/locating-visa-files-at-nara), фотографий семей американских индейцев в 1920-х годах в фондах Национальных Архивов (см. https://historyhub.history.gov/community/american-indian-records/blog/2020/07/06/1920s-photographs-of-american-indian-families-in-national-archives-holdings), защиты прав представителей LGBTQIA+ сообщества в федеральных судах (см. https://historyhub.history.gov/community/researchers-help/blog/2021/01/28/subject-matter-expert-sme-civil-rights-blog-1-lgbtqia-equal-protection-records-in-federal-courts) и до «20 советов по успешному исследованию материалов переписи населения» (см. https://historyhub.history.gov/community/genealogy/blog/2020/12/22/20-tips-for-census-research-success).

Центр изучения истории (History Hub) - это фантастический инструмент, который позволяет исследователям воспользоваться обширными знаниями справочно-исследовательской службы, касающимися документов в фондах Национальных Архивов.

Многочисленные подразделения справочно-исследовательской службы участвуют в проектах детализации архивного научно-справочного аппарата с тем, чтобы еще больше облегчить доступ к указателям и каталогам, добавляемый в Каталог Национальных Архивов (National Archives Catalog, https://catalog.archives.gov – *онлайн-система Национальных Архивов, обеспечивающая доступ к научно-справочному аппарату и к выложенным в свободном доступе оцифрованным архивным материалам*).



Генеалогическое сообщество на History Hub



На фото: карточка из картотеки «Послужные карточки санитаров, матрон и медсестер 1861–1865 гг.»

На сегодняшний день в рамках этих совместных проектов было создано почти три четверти миллиона описаний уровня документа для различных серий документов, включая Указатель получателей награды «Пурпурное сердце» (Purple Heart Award Recipients, https://catalog.archives.gov/id/6424319); «Каталог зарубежных врагов» (Alien Enemy Index, https://catalog.archives.gov/id/602456); «Именной указатель к корреспонденции Бюро натурализации (Name Index to Bureau of Naturalization Correspondence Files, https://catalog.archives.gov/id/1593296); «Послужные карточки санитаров, матрон и медсестер» (Carded Service Records of Hospital Attendants, Matrons and Nurses, https://catalog.archives.gov/id/655658); и «Картотеку смертей гражданских лиц» (Carded Death Records of Civilians, https://catalog.archives.gov/id/655728).

В прошлом месяце, как раз накануне Месячника афроамериканской истории (Black History Month), в Каталог Национальных Архивов были добавлены «Рассказы рабов» рассказов о рабах (Slave Narrative Files, https://catalog.archives.gov/id/649294), среди «Пожертвованных документов Центра городской этнологии (Center for Urban Ethnology, CUE) Пенсильванского университета». В состав этих электронных документов входят более 200 записей бесед, первоначально проведенных в период с 1936 по 1938 год Управлением общественных работ (Works Progress Administration, WPA - *независимое федеральное агентство, созданное в 1935 году по инициативе президента Рузвельта, ставшее основным в системе трудоустройства безработных в ходе осуществления рузвельтовского Нового курса*) и отперфорированных на перфокартах 80-колоночных перфокартах IBM исследователем из CUE д-ром Джеймсом Кахаланом (James Cahalan) в конце 1970-х годов. Д-р Кахалан использовал эти компьютеризированные интервью в своем лингвистическом исследовании, и передал их в дар Национальным Архивам в 2000 году. Отдел электронных документов принял переданные в качестве дара перфокарты, приобрел настольный считыватель перфокарт, а затем преобразовал информацию в ряд текстовых файлов формата ASCII.

Совместными усилиями Отделения видеоаудиоматериалов (Moving Image and Sound Branch) и Лаборатории обеспечения сохранности кинофильмов (Motion Picture Preservation Lab) через Каталог Национальных Архивов стала доступной серия великолепных черно-белых видеороликов из библиотеки архивных видеоматериалов, собранной Информационным агентством США (United States Information Agency, USIA. Вы также можете узнать дополнительную информацию об архивных фотографиях в составе данной библиотеки (Library Stock Shots, https://catalog.archives.gov/id/57921) и проекте по предоставлению доступа к этим материалам в посте (см. https://unwritten-record.blogs.archives.gov/2020/10/21/searchable-stock-shots-306-lss-films-now-online/) на блоге «Неписанная история» (Unwritten Record).

Помимо той невероятной работы, о которой я сказал выше, сотрудники внесли значительные усовершенствования в Каталог Национальных Архивов

с помощью тегов и транскрипции. Эти усилия улучшают результаты поиска по нашим документам и делают рукописный или трудночитаемый текст доступным для более широкой аудитории. В работе по маркировке и транскрибированию участвует больше сотрудников, чем когда-либо, и я благодарен каждому из них за то, что они делают наши документы легче отыскиваемыми и более доступными.

Снимок из фондов «библиотеки архивных видеоматериалов». Кадр из ед.хр. 306-LS-677, архивный шифр 58054, см. https://catalog.archives.gov/id/58054

Это лишь некоторые из множества способов, при помощи которых сотрудники Национальных Архивов США предоставляют доступ к нашим обширным фондам. Я ещё раз благодарю всех наших сотрудников, продолжающих обеспечивать доступ к архивным материалам и поддерживать связь с клиентами во время пандемии Covid-19. Я знаю, что наши клиенты, как и я, ценят Ваши усилия.

КАКИЕ ДОКУМЕНТЫ МЫ ДОЛЖНЫ ХРАНИТЬ НА БУМАГЕ? ГЛОБАЛЬНОЕ РУКОВОДСТВО ПО СОБЛЮДЕНИЮ ТРЕБОВАНИЙ К НОСИТЕЛЯМ ИНФОРМАЦИИ, МЕСТОНАХОЖДЕНИЮ И ПЕРЕДАЧЕ ДОКУМЕНТОВ

Источник: сайт ARMA International https://magazine.arma.org/2021/01/which-records-should-we-retain-in-paper-a-global-guide-to-media-location-and-transfer-compliance/

«Просто скажите мне, какие документы мы должны хранить на бумаге!» - это обычное проявление разочарования среди специалистов по управлению документами и полномасштабному управлению информацией. Лица, ответственные за ведение и представление документов, предпочитают сохранять и передавать свои документы с использованием наиболее эффективного метода хранения, но не хотят при этом нарушать закон, сохраняя информацию в незаконном формате.

Цель данной статьи – дать специалистам по управлению документами и информацией рекомендации, помогающие определить, какие документы они должны хранить в бумажном виде, а какие могут храниться в электронном виде. Такого рода анализ включает понимание того, как документы используются, - наряду с соответствующими законами и нормативными актами, затрагивающими управление документами.

По этой причине данная статья побуждает организации, сталкивающиеся с вопросом о хранении своих документов в глобальном масштабе в бумажном или электронном виде, учитывать следующие три фактора при принятии решения о том, на каких носителях сохранять документы:

- Правовая допустимость электронных документов;,
- Специфические требования к местонахождению документов;
- Национальные ограничения на передачу данных.

Помимо объяснения процесса определения того, какие документы организация должна хранить на бумаге, а какие могут храниться в электронном виде, в данной статье приведен высокоуровневый обзор нормативно-правовой базы США и ещё более 80 стран, помогающий исполнять законодательно-нормативные требования, связанные с носителями информации, местонахождением и передачей документов и информации.

Методология исследования

Представленная здесь информация является результатом глобального анализа законов и нормативных актов 80 стран, затрагивающих вопросы управления документами. В ходе исследования главное внимание уделялось

базовым законам и нормативным актам, регламентирующим хранение бухгалтерских, кадровых, налоговых и договорных документов.

В ходе анализа определялось, используется ли в нормативно-правовых актах язык, который указывает на то, какие носители информации могут или должны использоваться, и выявлялись требования, связанные с местонахождением и возможностью проверки этих документов. Также входе исследования обращалось внимание на то, допускают ли эти законы передачу данных, и изучались требования и ограничения на передачу данных, вытекающие из законов о защите неприкосновенности частной жизни и персональных данных. Исследование материалов по всем 80 странам проводилось в 2020 году.

Хранение документов в бумажном и электронном виде в США

В США в общем случае допускается создание и хранение информации в электронном виде, при условии, что сохраняется целостность информации. Под целостностью, как правило, понимается то, что содержащаяся в документах информация после их создания или получения не может быть изменена, и не может быть измён состав документов.

Есть несколько подразумеваемых по умолчанию исключений, когда документы должны сохраняться в исходном бумажном формате - это, например, документы о наследстве (завещания, доверенности на управление имуществом (trusts)); нотариально заверенные контракты с рельефными печатями; документы, подтверждающие право собственности (titles), и оборотные/обращающиеся кредитно-денежные инструменты (например, чеки и переуступаемые векселя). В этих исключительных случаях нет прямого требования сохранять документы в бумажном виде. Вместо этого есть понимание того, как используются эти документы и материалы, и осознаётся польза от их хранения на бумаге или в их первоначальной форме. Одно из правил, которым следует следовать в США, заключается в следующем: если ценность документа связана с владением этим документом, то Вам следует сохранять именно оригинал документа; отсканированной или электронной копии будет недостаточно.

Глобальный анализ: Допускаются ли электронные документы?

В зарубежном законодательстве редко прямо говорится, что документ должен сохраняться в бумажной форме. Напротив, когда допускается использование электронных документов, то в законах обычно прямо говорится о допустимости их использования или о допустимости использования любых носителей информации (включая электронные и бумажные). Почти в каждом случае, когда допускается использование электронных документов, закон или нормативный акт требует, чтобы (1) сохранялась целостность информации, и (2) организация была способна распечатать информацию.

Документы бухгалтерского учёта

Типичные документы бухгалтерского учёта с наибольшей вероятностью могут управляться в электронном виде. Ниже приводится разбивка 80 стран по категориям в зависимости от того, в какой мере их законодательство допускает хранение бухгалтерских документов в электронном формате.

В число стран, которые обычно разрешают хранение документов и материалов бухгалтерского учёта в электронном формате, входят:

Албания, Алжир, Аргентина, Армения, Австралия, Бразилия, Канада, Китай (КНР), Колумбия, Чехия, Дания, Финляндия, Габон, Гана, Греция, Гватемала, Индия, Индонезия, Ирландия, Италия, Япония, Иордания, Казахстан, Кения, Косово, Литва, Люксембург, Мадагаскар, Малайзия, Норвегия, Панама, Филиппины, Польша, Португалия, Румыния, Россия, Саудовская Аравия, Сингапур, Словакия, Южная Африка, Южная Корея, Испания, Шри Ланка, Швеция, Швейцария, Тайвань, Турция, Уганда, Украина, Объединенные Арабские Эмираты, Великобритания, Узбекистан и Вьетнам.

В число стран, которые разрешают хранение документов и материалов бухгалтерского учёта в электронной форме, однако требуют, чтобы эта форма была «оригинальной», той, в которой документ или материал был создан, входят:

Босния, Доминиканская Республика, Франция, Грузия, Германия, Мексика, Черногория и Сербия.

В число стран с уникальными требованиями к электронным документам и материалам бухгалтерского учёта, входят:

- Сальвадор, где требуется получать предварительное разрешение на хранение документов в электронном формате;
- Голландия, где требуется хранить в бумажном виде бухгалтерский баланс (Balance Sheet) и отчеты о финансовых результатах деятельности (Profit and Loss Account Income Statements), но разрешается хранить все остальные бухгалтерские документы в электронном виде.

В число стран, которые не разрешают хранение документов и материалов бухгалтерского учёта в электронном виде или же прямо требуют хранить их бумажные экземпляры, входят:

Чили, Египет, Эфиопия, Монголия, Марокко, Таиланд и Тунис.

В число стран, в законодательстве которых о бухгалтерском учете отсутствуют требования к носителям информации, входят:

Камбоджа, Коста-Рика, Гайана, Ямайка, Ливан, Нигерия, Перу, Сьерра-Леоне, Суринам и Танзания.

Обзор по 80 странам показывает, что в большинстве стран допускается электронное хранение бухгалтерских документов. Десять стран никак не регламентируют этот вопрос, а семь стран требуют, чтобы информация хранилась в бумажном виде (формулировки вроде «сшитые книги и журналы») и не допускают хранение документов бухгалтерского учёта в электронном виде.

Ещё в восьми странах разрешено хранение бухгалтерских документов в электронном виде, но только в том электронном формате, в котором документ был изначально создан. По сути, это требование о том, чтобы организации сохраняли сведения бухгалтерского учёта в их исходной форме, что может включать их сохранение в исходном компьютерном формате (например, в Германии).

Документы налогового учёта

Хотя относящимся к налоговому учёту документам в тех же странах могут устанавливаться иные сроки хранения, и эти документы могут использоваться для иных целей, - требования к носителям информации для них аналогичны требованиям к бухгалтерским документам. Фактически, во многих случаях законы и нормативные акты о налоговом учёте по вопросам использования носителей информации ссылаются на законы и нормативные акты о бухгалтерском учёте.

В Евросоюзе для счетов-фактур, отражающих налогом на добавленную стоимость, может потребоваться краткосрочное хранение бумажных оригиналов с целью получения возмещения НДС. В соответствии с Тринадцатой директивой Совета Европы 86/560/EEC (см. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31986L0560), возможно возмещение НДС, уплаченного налогоплательщики, зарегистрированными вне территории Евросоюза. Многие стран-члены Евросоюза требуют предоставления оригиналов счетов-фактур для получения полагающегося возмещения НДС.

Контракты

За некоторыми исключениями, законы и нормативные акты не требуют сохранения контрактов. Хотя сохранение контрактов имеет смысл для анализа обязательств и снижения судебных рисков, в то же время решение о сохранении такой информации является исключительно деловым решением.

Таким образом, вопрос о том, что сохранять – бумажный экземпляр или отсканированную электронную копию - также является деловым решением. В некоторых случаях оригинальные / бумажные экземпляры имеют дополнительную ценность. В качестве примеров можно назвать контракты с печатями, аннотациями или рукописными пометками; или же контракты, которые могут быть переуступлены. Другие виды контрактов, такие, как заказы на поставку или большинство технических заданий, не имеют особой ценности в их бумажной / оригинальной форме, при условии, что сохраняется целостность документа.

Документы о трудовой деятельности и занятости

Если обычно в целом понятно, можно ли хранить в электронном виде документы бухгалтерского и налогового учёта, то вопрос о возможности использования электронных документов о трудовой деятельности (например,

платежных ведомостей, кадровых дел, документов об охране труда и здоровья на рабочем месте и о несчастных случаях) более неоднозначен.

Например, когда речь идёт о документах о несчастных случаях, в законодательстве, скорее всего, будет назван определенный формат (форма), а не вид носителя. Если форма существует и может быть заполнена в электронном виде, то разумно предположить, что Вы можете сохранять её в электронном формате. Если, однако, все формы являются бумажными, то разумно предположить, что Вы должны будете сохранять сведения о несчастном случае в бумажной форме.

Ниже приводится разбивка 80 стран по категориям в зависимости от того, допускает ли их законодательство электронное хранение документов о заработной плате.

В число стран, которые обычно разрешают хранение документов и материалов о заработной плате в электронном формате, входят:

Албания, Армения, Австралия, Босния, Канада, Китай (КНР), Чехия, Дания, Сальвадор, Франция, Германия, Греция, Ирландия, Италия, Казахстан, Кения, Косово, Литва, Мадагаскар, Малайзия, Мексика, Черногория, Марокко, Нидерланды, Перу, Польша, Румыния, Сербия, Сьерра-Леоне, Сингапур, Южная Африка, Южная Корея, Испания, Швейцария, Тайвань, Объединенные Арабские Эмираты, Великобритания и Вьетнам.

В число стран, которые разрешают хранение документов и материалов о заработной плате в электронной форме, но требуют, чтобы эта форма была «оригинальной», в которой документ или материал была создан, входят:

Аргентина, Грузия и Индия.

В число страны с уникальными требованиями к электронному хранению документов и материалов о заработной плате, входят:

- Люксембург, где требуется хранить данные о заработной плате в «Специальном регистре», и
- Норвегия, где требуется хранить информацию как в бумажной, так и в электронной форме.

В число стран, которые не разрешают электронное хранение документов и материалов о заработной плате, или же отдают предпочтение бумажным документам, входят:

Бразилия, Камбоджа, Колумбия, Коста-Рика, Доминиканская Республика, Филиппины, Россия, Словакия, Шри-Ланка, Украина и Узбекистан.

В число стран, в законодательстве которых о зарплатных документах отсутствуют требования к носителям информации, входят:

Алжир, Чили, Египет, Эфиопия, Финляндия, Габон, Гана, Гватемала, Гайана, Индонезия, Ямайка, Япония, Иордания, Ливан, Монголия, Нигерия, Панама, Португалия, Саудовская Аравия, Швеция, Суринам, Танзания, Таиланд, Тунис, Турция и Уганда.

Обзор по 80 странам показывает, что в отношении зарплатных документов многие страны либо разрешают электронное хранение таких документов, либо не упоминают этот вопрос в своём трудовом законодательстве. Однако 16 из 80 стран или требуют хранения документов о заработной плате на бумаге, или выставляют особые требования, предусматривающие хранение в оригинальном формате, в специальных регистрах, или одновременно в бумажном и в электронном виде.

Требования к местонахождению

В отношении некоторых видов документов существуют явные требования к местонахождению, а в отношении некоторых другие – неявные требования такого рода. Примером явных требований к местонахождению может служить требование о том, чтобы документы или материалы находились по месту основной деятельности или занятости. Примером неявного требования является требование о том, чтобы документ был доступен для немедленной проверки. Анализ этих требований влияет на решение о сохранении информации в электронном или бумажном формате.

Документы бухгалтерского учёта

Как правило, цель бухгалтерского учета - защитить инвесторов и владельцев компании. Как следствие, местонахождение документов бухгалтерского учёта определяется уставными документами компании или наиболее простым способом передать эту информацию владельцам/акционерам. Электронные документы обычно не препятствуют достижению этой цели, пока обеспечивается доступность информации.

Документы налогового учёта

Власти проверяют документы налогового учёта для целей аудита и обеспечения их соответствия информации, представленной в налоговых декларациях. Это не «точечные» или «внезапные» проверки. Как правило, организации получают уведомление и им даётся время на то, чтобы собрать информацию из своих первоисточников и распечатать её. Единственным исключением из этого правила могут быть таможенные документы, относящиеся к налогам, связанным с таможенными пошлинами.

Контракты

Контракты обычно не проверяются властями; это частные соглашения. Однако, поскольку они являются частными соглашениями, иногда на них распространяются законы о защите персональных данных. В некоторых странах, таких как Китай и Россия, существуют строгие ограничения на местонахождение персональных данных. В большинстве других стран, следуя примеру Евросоюза, имеются ограничения на передачу персональных данных. Эти ограничения рассматриваются ниже.

Документы о труде и занятости, включая документы об охране труда и здоровья на рабочем месте

Документы такого рода с наибольшей вероятностью могут потребоваться для немедленной проверки. В их число могут попасть сведения о заработной плате, персонале, несчастных случаях, иные сведения

об охране труда и здоровья, связанные с трудовой деятельностью. Законы и нормативные акты о труде обычно требуют, чтобы такая информация была доступна для немедленной проверки. Если документ недоступен ввиду того, что он находится в электронной системе и не может быть своевременно распечатан и/или представлен, организация будет оштрафована и/или будут иные неприятные последствия. В результате организации могут решить, что более эффективно хранить эти документы в бумажном формате по занятости.

Ограничения на передачу

В соответствии с законодательством Евросоюза и стран, установивших аналогичные требования, персональные данные не могут передаваться в другие страны, если эти страны не обеспечивают для них равноценный уровень защиты. Соединенные Штаты не обеспечивают такой равноценной защиты, что делает передачу персональных данных в США из многих стран незаконной, если только не будут предприняты определенные действия или меры предосторожности (например, представление Обязывающих корпоративных правил (Binding Corporate Rules) или соответствие Стандартным условиям договора (Standard Contract Clauses)).

Эта позиция была усилена в июле 2020 года, когда Европейский суд (European Court of Justice) постановил, что программа «Щит, защищающий неприкосновенность частной жизни» (Privacy Shield - *соглашение о взаимной защите персональных данных между США и Евросоюзом*), использовавшаяся многими американскими организациями для передачи персональных данных граждан Евросоюза в США, неадекватна для защиты информации граждан Евросоюза и, следовательно, её незаконно использовать для обеспечения соответствия европейскому законодательству о защите персональных данных (GDPR). (Дело C-311/18 «Еврокомиссар по защите персональных данных против Facebook Ireland и Maximillian Schrems, 16 июля 2020 года).

Следовательно, если компания хранит персональные данные в корпоративной системе управления контентом, размещённой в облаке, и эти персональные данные доступны в США, то организация может нарушать некоторые законы о защите персональных данных. Это обстоятельство может повлиять на решение использовать такие электронные системы для хранения персональных данных.

Еще одна проблема, связанная с передачей данных, - это миграция данных из одной системы в другую или сканирование аналоговых документов в электронные версии. Как мы уже показали, многие законы и нормативные акты допускают использование как электронных, так и бумажных версий документов, но при этом требуют сохранения оригинальной версии. Это означает, что если документ создается в бумажной форме, он должен сохраняться в исходной бумажной форме; если же документ создается в электронной системе, то он должен оставаться в той же электронной системе.

Выводы

Большинство стран допускают использование электронных документов, - но какой бы метод хранения ни использовался, этот метод должен обеспечивать сохранение целостности информации, её доступность и возможность распечатать при необходимости.

Организации должны быть особенно осторожны с трудовыми документами, персональными данными и документами, ценность которых заключается в обладании оригиналом.

Возможны ситуации, когда организации хранят информацию в двух системах: экземпляр в корпоративной системе для внутренних целей; и бумажную версию, на случай проверок и во исполнение законодательно-нормативных требований – на территории компании или в иных допустимых местах. Это не то же самое, что хранение бумажных дубликатов во внеофисных хранилищах, поскольку такое хранение вне местоположения организации не решает задачу предоставления документов для немедленной проверки. Следовательно, подобную практику не следует поощрять.

Изучив законодательство на предмет допустимости электронного хранения, наличия явных и неявных требования к местонахождению и ограничений на передачу документов, организация сможет принять обоснованное решение о том, какие документы ей следует хранить в электронном, и какие - в бумажном виде.

КАРЛ МЕЛРОУЗ: МЫ НЕ МОЖЕМ СНАЧАЛА СКАЗАТЬ ДЕЛОВЫМ ПОДРАЗДЕЛЕНИЯМ, ЧТО ОНИ - ХРАНИТЕЛИ СВОИХ ДОКУМЕНТОВ, А ЗАТЕМ - ЧТО ЭТО НЕ ИХ ДОКУМЕНТЫ

Источник: блог «Стратегическое управление информацией» (Information Governance) https://informationgovernance.blog/2021/03/01/we-cant-tell-business-units-that-they-are-the-custodians-of-their-records-and-then-tell-them-that-theyre-not-their-records/
Автор: Карл Мелроуз

Это странная дихотомия, с которой я постоянно сталкивался в течение нескольких последних лет (*в контексте данного поста понятия «дихотомия» означает взаимоисключающие*).

Когда я беседую с представителями групп управления документами, те нередко говорят мне, что не несут ответственности за качество документов в системе, потому что ответственными хранителями документов являются деловые подразделения.

Затем эти люди, в свою очередь, разговаривают со специалистами подобного делового подразделения, которое не делает то, чего требует от него группа управления документами, - и говорят им, что документы не их, что они принадлежат организации.

Так какое из этих высказываний соответствует реальности?

И каковы предсказуемые последствия такого варианта?

Поставлен интересный вопрос – но он не учитывает возможности того, что оба противопоставляемых утверждения могут быть верны одновременно.

Организация, которая практически всегда по закону является собственником своих деловых документов, вполне может передать их в оперативное управление конкретным подразделениями и лицам, дав им права ответственных хранителей, но не отказываясь при этом от своих прав собственника – в том числе и права определять принципы (в первую очередь стратегические) и порядок управления документами.

Если возникают подобные споры, то для их разрешения необходимо, чтобы, с одной стороны, служба управления документами, выступающая от лица организации-собственника, понимала особенности деятельности делового подразделения, в том числе затраты, отдачу и риски, связанные с исполнением подразделением устанавливаемых службой требований – которые вполне могут оказаться неоправданно трудозатратными.

Со своей стороны, подразделение-хранитель должно осознавать, что ему доверено формирование, ведение и хранение корпоративного актива, а не их личной кучки документов – и, соответственно, всё это надо делать в соответствии с существующими законодательно-нормативными требованиями, деловыми и иными требованиями самой организации и сложившейся корпоративной культурой. Такому осознанию может способствовать, в частности, выдача «пряников» за качество ведения ресурса, а не использование одного только «кнута» за неисполнение требований.

КАРЛ МЕЛРОУЗ: ПРАКТИКА УПРАВЛЕНИЯ ДОКУМЕНТАМИ БЕЗ ФИЗИЧЕСКОГО КОНТРОЛЯ НАД НИМИ, ПОДТВЕРЖДАЕМАЯ ФАКТАМИ

Источник: блог «Стратегическое управление информацией» (Information Governance) https://informationgovernance.blog/2021/03/03/evidence-based-non-custodial-records-management/

Управление документами - это профессия с тысячелетней историей. Или, по крайней мере, управление документами в условиях, когда те

находятся под полным физическим и интеллектуальным контролем соответствующей стороны (кастодиальное управление документами - custodial records management).

Однако управление документами в отсутствии физического контроля над ними (некастодиальное управление документами - non-custodial records management) - это совсем другое дело.

Этот подход повседневно практикуется в системах, которые не были на это рассчитаны, и людьми, которые его не понимают или не хотят понять.

Так где же наши факты, касающиеся того, как мы выполняем свои профессиональные обязанности в подобных условиях?

Чем больше я читаю, тем больше вижу, как переосмысливаются старые идеи.

Проблема здесь заключается в том, что старые идеи были основаны на старой экономике, а новые идеи основаны на представлениях об удобстве, в которые или мы не верим, или которые просто не работают.

Вот три примера:

- На наши представления о проведении уничтожения влияет экономический факт стоимости хранения короба с документами в 5 австралийских долларов в месяц. Остаются ли осмысленными эти представления тогда, когда стоимость хранения «электронного эквивалента» короба с документами в течении 100 лет составляет менее 1 доллара?
- Установление срока хранения и определение действий по его истечении в момент создания документа посредством интеграции деловой классификационной схемы и перечня видов документов с указанием сроков хранения - идея, которая вроде бы повсеместно внедрялась на практике. Я, однако, обнаружил, что лишь 2 из 100 организаций доверяют ей в достаточной степени, чтобы действительно уничтожать документы на основе такого решения, а все остальные проводят дополнительную экспертизу вручную – платя специалистам более 25 долларов за час.
- Иерархия «функция - вид деятельности – деловая операция/транзакция» (function-activity-transaction, FAT – *традиционная формула популярного в Австралии функционального подхода к систематизации документов*) является золотым стандартом при разработке классификационных схем, - но обеспечивает ли этот подход более высокое качество документов? По моему собственному опыту могу сказать, что классификационные схемы часто являются серьёзным препятствием для эффективного использования документных систем.

Где доказательства того, какие из подходов реально работают?

Сколько из того, что мы делаем сейчас по умолчанию, является скорее догмой, чем эффективной практикой, подтверждаемой фактами?

КАРЛ МЕЛРОУЗ: ЯДОВИТЫЕ ВОПРОСЫ

Источник: блог «Стратегическое управление информацией» (Information Governance) https://informationgovernance.blog/2021/03/10/how-useful-is-the-evidence-that-we-are-keeping/
https://informationgovernance.blog/2021/03/08/why-do-we-bother-with-compliance-is-mandatory/

Насколько полезны хранимые нами документальные доказательства?

Я полагаю, что это полезный вопрос, который должен иметь в виду каждый специалист по управлению документа, когда он решает, как расставить приоритеты проектов и мероприятий.

Проблема с этим вопросом заключается в том, что он всегда интерпретируется субъективно, поэтому я предлагаю следующие категории:

- Документы, которые потенциально полезны неустановленному лицу для неизвестной потребности в неизвестное время в будущем;
- Документы, которые, вероятно, будут полезны для удовлетворения конкретной потребности в неизвестное время в будущем;
- Документы, полезные для удовлетворения постоянно существующей конкретной потребности.

Быстро становится очевидным, где нам следует в первую очередь приложить усилия.

Как при оценке рисков, здесь важна не только вероятность/частота использования документов, но и «цена вопроса». Без этого есть риск не уделить должного внимания тем документам, которые, возможно и не понадобятся – но уж если понадобятся, то для решения очень важных вопросов, таких. например, как отстаивание прав собственности на ценные активы.

Зачем мы продолжаем настаивать, что «исполнение наших требований сотрудниками является обязательным»?

Если мы сами и наша организация не относится к этому абсолютно серьёзно, то в итоге мы просто выглядим глупо.

Вот как можно узнать, серьезно ли относится Ваша организация к соблюдению установленных требований:

- Ваши документы в идеальном порядке;
- Вам известно количество случаев несоблюдения требований;
- Людей увольняли за неисполнение требований.

Кому-нибудь довелось когда-нибудь работать в такой организации?

Контроль над соблюдением требований (даже в узкой трактовке – требований к управлению документами) никогда не надо доводить до абсурда. Не секрет, что в наше время быстрых перемен нормативная база и содержащиеся в ней требования стремительно устаревают; попытка

строго эти требования соблюдать может привести к фактическому саботажу основной деятельности организации.

По опыту, идеальный порядок редко когда возможен в живой оперативной деятельности; он чаще встречается в умирающих органах и организациях.

Опыт опять-таки показывает, что увольнять людей имеет смысл лишь в крайних случаях – иначе легко можно разбазарить ценные кадры (а реже всего ошибается тот, кто ничего не делает), да и поговорка о том что «за одного битого двух небитых дают» тоже не просто так появилась. Увольнения часто не столько признак успешной борьбы за порядок в организации, сколько свидетельство провалов в работе с кадрами (в том числе и со стороны службы управления документами).

КАРЛ МЕЛРОУЗ: ПОЧЕМУ МЫ ГОВОРИМ ОБ УПРАВЛЕНИИ ИНФОРМАЦИЕЙ КАК АКТИВОМ, ЕСЛИ ОНА ПО БОЛЬШЕЙ ЧАСТИ ТАКОВЫМ НЕ ЯВЛЯЕТСЯ?

Источник: блог «Стратегическое управление информацией» (Information Governance) https://informationgovernance.blog/2021/03/17/why-do-we-talk-about-managing-information-as-an-asset-when-most-of-our-information-isnt/

Управление информацией как активом - идея не новая, но у меня есть серьезные проблемы с её осуществлением на практике.

На языке бухгалтерского учета, для того, чтобы считать нечто активом, мы должны ожидать в будущем приток в организацию, благодаря ему, денежных поступлений.

Итак, какая часть хранимой нами информации действительно является «активом»?

Кто-нибудь когда-нибудь делал прогнозы доходов от своей информации?

Если информация не будет приносить денежных поступлений (или поддерживать экономию затрат), - разве это не делает её обузой?

Пользователь Chel так прокомментировал этот пост:

«Возможно, именно поэтому об управлении документами всё чаще говорят с точки зрения менеджмента риска? Раз менеджмент риска рассматривается как «необходимое бремя», то и управление документами можно считать аналогичной формой страховки».

На это Карл Мелроуз ответил следующее:

«Об этом можно было бы вести очень долгий разговор. Я думаю, что подход на основе менеджмента риска опасен для управления документами,

потому что в него по-настоящему вкладываются только сразу после того, как случается какой-то инцидент, - и проблема здесь в том, что даже после того, как что-то подобное случилось, никто не хочет инвестировать в ликвидацию последствий всего того, что происходило ранее ... они лишь хотят сказать: «Начиная с этого момента, мы будем вести хорошие документы». Конечным результатом является паршивое качество документов, и, как следствие, наша профессиональная деятельность недооценивается.

Я считаю, что нам нужно удвоить внимание к аспекту деловой полезности нашей деятельности, потому что это единственное, что даёт стабильную, проверяемую, измеримую и очевидную отдачу. Однако измерить деловую полезность / отдачу сложно, и специалистов по управлению документами этому не учат – соответственно, они об этом и не задумываются. Поэтому я думаю, что существует проблема как специалистов, которые не знают, как распознать, когда их деятельность даёт отдачу, - так и проблема того, что эти специалисты не знают и не умеют измерять эту отдачу и информировать о ней.

Вот простой пример: Специалист по управлению документами, с которым я разговаривал на прошлой неделе, только что переименовал заголовки целой серии дел, чтобы они соответствовали требованиям другой системы. Каждую неделю они получали от 15 до 20 запросов в связи с тем, что сотрудники не могли найти документы самостоятельно, и поэтому обращались за помощью в группу управления документами. Он переименовал всю серию дел ради того, чтобы в этом больше не было необходимости. Это очень полезная работа, но проблема в том, что он не подумал об этом заранее с данной точки зрения, поэтому и не задокументировал объём запросов, трудозатраты на поиск (как сотрудников деловых подразделений, так и персонала его собственной группы); и не написал экономического обоснования для выполнения подобной работы – соответственно, эта отдача осталась невидимой для организации, пусть даже на самом деле она очень существенно способствовала повышению производительности труда, вследствие чего со временем организация сэкономит массу денег.

Я думаю, нам нужно сосредоточиться на такого рода усилиях. У нас нет времени на это, но это потому, что у нас недостаточно людей - поэтому нам необходимо начать уделять время данным усилиям, чтобы показать свою ценность, получить больше людей - и получить время для этих усилий.

А что думаете Вы?»

МЕЖДУНАРОДНЫЙ СОВЕТ АРХИВОВ ПРОВОДИТ 7-11 ИЮНЯ МЕЖДУНАРОДНУЮ НЕДЕЛЮ АРХИВОВ 2021 ГОДА С ТЕМОЙ «РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ АРХИВОВ»

Источник: сайт МСА https://www.ica.org/en/international-archives-week-7-11-june-2021-empoweringarchives

С понедельника 7 июня по пятницу 11 июня 2021 года мы будем отмечать третью Международную неделю архивов (International Archives Week, IAW2021), и в этом году основной темой будет «Расширение возможностей архивов» (Empowering Archives).

Мы приглашаем организации и специалистов в области архивного дела и управления документами присоединиться к нам в виртуальном обсуждении темы «Расширение возможностей архивов».

МСА проведёт торжественное открытие Международной недели архивов **31 марта 2021 года**. Это мероприятие - возможность узнать о второй кампании МСА в социальных сетях и о Международной недели архивов 2021 года, построенной на основе темы «Расширение возможностей архивов»; о том, как мы будем использовать соответствующие хештеги **#EmpoweringArchives** и **#IAW2021**.

Оно также даст возможность обсудить, как архивы укрепляют и поддерживают подотчетность и прозрачность посредством предоставления доступа к информации с целью привлечения к ответственности правительств и обеспечения гражданам возможности защищать свои права; или же как взаимодействие и сотрудничество позволяют нам расширять возможности архивов и профессии в целом, помогая нам в достижении наших целей и решении задач, стоящих перед профессией и нашими организациями благодаря поддержке представителей смежных профессий, одновременно помогая другим секторам и широкой общественности понять, что именно мы делаем. И, наконец, мы хотели бы обсудить, как бросить вызов существующей архивной теории и практике, чтобы сделать их более многообразными и инклюзивными в отношении разных голосов и разных историй.

Примите участие в этой дискуссии о расширении возможностей архивов и в праздновании Международной недели архивов 2021 года. Ваши голоса важны для нас и для всей профессии!

Чтобы получить дополнительную информацию, следите за публикациями на нашем веб-сайте (https://www.ica.org/en), в новостной рассылке (https://www.ica.org/en/public-resources/newsletters) и в социальных сетях Twitter (https://twitter.com/icarchiv) и Facebook (https://www.facebook.com/ICAInternationalCouncilonArchives/)!

ЗМІСТ